



ADSL 2/2+ VPN Firewall Router

ADE-4300A/B, ADW-4300A/B

User's Manual

Copyright

Copyright© 2005 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution:

To assure continued compliance (example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this Device must accept any interference received, including interference that may cause undesired operation.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

Revision

**User's Manual for PLANET ADSL 2/2+ VPN Firewall Router, 802.11g Wireless
PLANET ADSL 2/2+ VPN Firewall Router
Model: ADE-4300A/B, ADW-4300A/B
Rev: 1.0 (Jan. 2005)
Part No. EM-ADE4300_ADW4300v4**

Table of Contents

CHAPTER 1 INTRODUCTION	1
ADE-4300/ADW-4300 Features.....	1
Package Contents	5
Physical Details	6
CHAPTER 2 INSTALLATION	8
Requirements.....	8
Procedure	8
CHAPTER 3 SETUP	10
Overview	10
Configuration Program	12
Setup Wizard.....	13
Home Screen.....	15
LAN Screen	16
Wireless Screen (ADW-4300 only)	18
Wireless Security (ADW-4300 only).....	21
Trusted Wireless Stations (ADW-4300 only)	23
Password Screen.....	25
Mode Screen	26
CHAPTER 4 PC CONFIGURATION	27
Overview	27
Windows Clients.....	27
Macintosh Clients	38
Linux Clients	38
Other Unix Systems	38
Wireless Station Configuration (ADW-4300 only)	39
Wireless Configuration on Windows XP (ADW-4300 only)	39
CHAPTER 5 OPERATION AND STATUS	49
Operation - Router Mode	49
Status Screen.....	49
Connection Status - PPPoE & PPPoA	53
Connection Details - Dynamic IP Address.....	54
Connection Details - Fixed IP Address	56
CHAPTER 6 ADVANCED FEATURES	57
Overview	57
Access Control	57
Internet.....	59
Dynamic DNS (Domain Name Server)	64
Firewall Rules	66
Firewall Services	71
Options	73
Schedule.....	74
Virtual Servers	76
VPN (IPSec)	75
Microsoft VPN	84
SNMP	98
CHAPTER 7 ADVANCED ADMINISTRATION	99
Overview	99
PC Database.....	100
Config File	104
Logging.....	105
E-mail.....	107

Diagnostics	109
Remote Administration	110
Routing	112
Upgrade Firmware	116
CHAPTER 8 MODEM MODE	117
Overview	117
Management Connections	117
Home Screen	118
Mode Screen	119
Operation	119
Status Screen	120
APPENDIX A TROUBLESHOOTING	122
Overview	122
General Problems	122
Internet Access	122
Wireless Access (ADW-4300 only)	123
APPENDIX B ABOUT WIRELESS LANS(ADW-4300 ONLY).....	125
Modes	125
BSS/ESS	125
Channels	126
WEP	126
WPA-PSK	126
Wireless LAN Configuration	127
APPENDIX C ABOUT VPNS	128
Overview	128
Common VPN Situations	130
VPN Example	131
APPENDIX D SPECIFICATIONS	135
ADSL 2/2+ VPN Firewall Router	135
Wireless Interface (ADW-4300 only)	136
Regulatory Approvals	137

Chapter 1

1

Introduction

This Chapter provides an overview of the ADE-4300/ADW-4300's features and capabilities.

Congratulations on the purchase of your new ADE-4300/ADW-4300. The ADE-4300/ADW-4300 is a multi-function device providing the following services:

- **ADSL 2/2+ Modem.**
- **Shared Broadband Internet Access** for all LAN users.
- **Wireless Access Point** for 802.11b and 802.11g Wireless Stations. (ADW-4300 only)
- **VPN Gateway** to allow secure VPN connections over the Internet.
- **4-Port Switching Hub** for 10BaseT or 100BaseT connections.

Wireless LAN

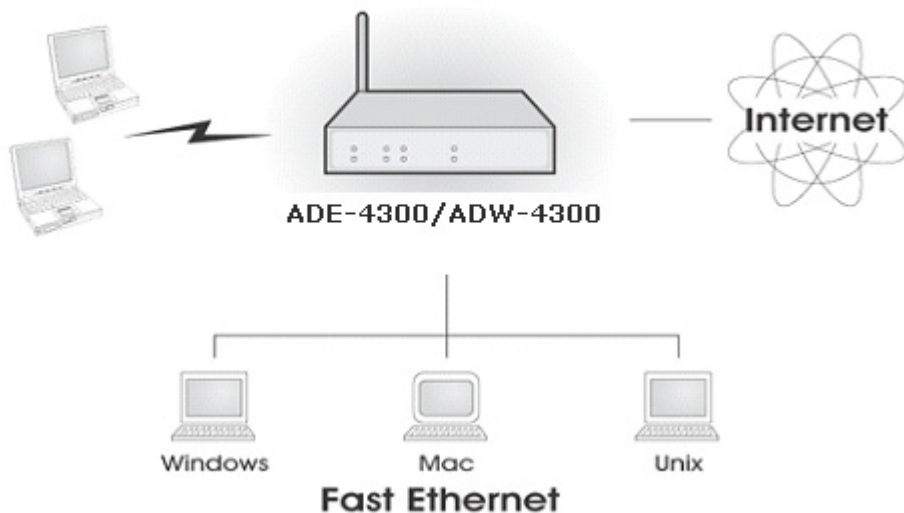


Figure 1: ADE-4300/ADW-4300

ADE-4300/ADW-4300 Features

The ADE-4300/ADW-4300 incorporates many advanced features, carefully designed to provide sophisticated functions while being easy to use.

Internet Access Features

- **Shared Internet Access.** All users on the LAN or WLAN can access the Internet through the ADE-4300/ADW-4300, using only a single external IP Address. The local (invalid) IP Addresses are hidden from external sources. This process is called NAT (Network Address Translation).
- **Built-in ADSL 2/2+ Modem.** The ADE-4300/ADW-4300 has a built-in ADSL 2/2+ modem, supporting all common ADSL 2/2+ connections.

- **IPoA, PPPoE, PPPoA, Direct Connection Support.** The ADE-4300/ADW-4300 supports all common connection methods.
- **Auto-detection of Internet Connection Method.** In most situations, the ADE-4300/ADW-4300 can test your ADSL and Internet connection to determine the connection method used by your ISP.
- **Fixed or Dynamic IP Address.** On the Internet (WAN port) connection, the ADE-4300/ADW-4300 supports both Dynamic IP Address (IP Address is allocated on connection) and Fixed IP Address.

Advanced Internet Functions

- **Application Level Gateways (ALGs).** Applications which use non-standard connections or port numbers are normally blocked by the Firewall. The ability to define and allow such applications is provided, to enable such applications to be used normally.
- **Special Applications.** This feature, also called Port Triggering, allows you to use Internet applications which normally do not function when used behind a firewall.
- **Virtual Servers.** This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.
- **URL Filter.** Use the URL Filter to block access to undesirable Web sites by LAN users.
- **Logs.** Define what data is recorded in the Logs, and optionally send log data to a Syslog Server. Log data can also be E-mailed to you.
- **Access Control.** Allows administrators to restrict the Internet Access available to PCs on your LAN.
- **Firewall.** As well as the built-in firewall to protect your LAN, you can define Firewall Rules to determine which incoming and outgoing traffic should be permitted.
- **Universal Plug and Play (UPnP)** UPnP allows automatic discovery and configuration of the Broadband Router. UPnP is supported by Windows ME, XP, or later.
- **Dynamic DNS Support.** DDNS, when used with the Virtual Servers feature, allows users to connect to Servers on your LAN using a Domain Name, even if you have a dynamic IP address which changes every time you connect.
- **Scheduling.** Both the URL Filter and Firewall rules can be scheduled to operate only at certain times. This provides great flexibility in controlling Internet-bound traffic.
- **VPN Connectivity.** Supports up to 8 IPSec VPN with DES, 3DES encryption and SHA-1 / MD5 authentication, the network traffic over public Internet is secured.
- **PPTP Server.** The ADE-4300/ADW-4300 emulates a Microsoft PPTP VPN Server, allowing clients to use the Microsoft VPN client provided in Windows.
- **VPN Pass through Support.** PCs with VPN (Virtual Private Networking) software using PPTP, L2TP and IPSec are transparently supported - no configuration is required.

Wireless Features (ADW-4300 only)

- **Standards Compliant.** The ADW-4300 complies with the IEEE802.11g (DSSS) specifications for Wireless LANs.

- **Supports both 802.11b and 802.11g Wireless Stations.** The 802.11g standard provides for backward compatibility with the 802.11b standard, so both 802.11b and 802.11g Wireless stations can be used simultaneously.
- **Speeds to 54Mbps.** All speeds up to the 802.11g maximum of 54Mbps are supported.
- **WEP support.** Support for WEP (Wired Equivalent Privacy) is included. Key sizes of 64 Bit and 128 Bit are supported. WEP encrypts any data before transmission, providing protection against snoopers.
- **WPA-PSK support.** Like WEP, WPA-PSK encrypts any data before transmission, providing protection against snoopers. The WPA-PSK is a later standard than WEP, and provides both easier configuration and greater security than WEP.
- **Wireless MAC Access Control.** The Wireless Access Control feature can check the MAC address (hardware address) of Wireless stations to ensure that only trusted Wireless Stations can access your LAN.
- **Simple Configuration.** If the default settings are unsuitable, they can be changed quickly and easily.

LAN Features

- **4-Port Switching Hub.** The ADE-4300/ADW-4300 incorporates a 4-port 10/100BaseT switching hub, making it easy to create or extend your LAN.
- **DHCP Server Support.** Dynamic Host Configuration Protocol provides a dynamic IP address to PCs and other devices upon request. The ADE-4300/ADW-4300 can act as a **DHCP Server** for devices on your local LAN and WLAN.

Configuration & Management

- **Easy Setup.** Use your WEB browser from anywhere on the LAN or WLAN for configuration.
- **Configuration File Upload/Download.** Save (download) the configuration data from the ADE-4300/ADW-4300 to your PC, and restore (upload) a previously-saved configuration file to the ADE-4300/ADW-4300.
- **Remote Management.** The ADE-4300/ADW-4300 can be managed from any PC on your LAN or Wireless LAN. And, if the Internet connection exists, it can also (optionally) be configured via the Internet.
- **Network Diagnostics.** You can use the ADE-4300/ADW-4300 to perform a *Ping* or *DNS lookup*.

Security Features

- **Password - protected Configuration.** Password protection is provided to prevent unauthorized users from modifying the configuration data and settings.
- **Wireless LAN Security. (ADW-4300 only)** WPA-PSK, WEP and Wireless access control by MAC address are all supported. The MAC-level access control feature can be used to prevent unknown wireless stations from accessing your LAN.
- **NAT Protection.** An intrinsic side effect of NAT (Network Address Translation) technology is that by allowing all LAN users to share a single IP address, the location and even the existence of each PC is hidden. From the external viewpoint, there is no network, only a single device - the ADE-4300/ADW-4300.

- **Firewall.** All incoming data packets are monitored and all incoming server requests are filtered, thus protecting your network from malicious attacks from external sources.
- **Protection against DoS attacks.** DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. The ADE-4300/ADW-4300 incorporates protection against DoS attacks.

Package Contents

The following items should be included. If any of these items are damaged or missing, please contact your dealer immediately.

- The ADE-4300/ADW-4300 Unit
- Quick Installation Guide
- User's Manual CD
- Power Adapter
- 1 RJ-45 Cable
- 1 RJ-11 (ADSL) cable

Physical Details

Front-mounted LEDs of ADE-4300



Figure 2: Front Panel of ADE-4300

Front-mounted LEDs of ADW-4300

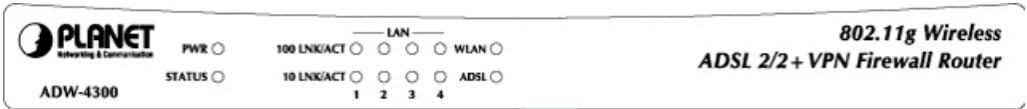


Figure 3: Front Panel of ADW-4300

PWR LED	On - Power on. Off - No power.
STATUS LED	Off - Normal operation. Blinking - This LED blinks during start up, and during a Firmware Upgrade.
LAN LED	For each port, there are 2 LEDs, to indicate the connection speed (10BaseT or 100BaseT) of each port. <ul style="list-style-type: none">• 100 LNK/ACT - This will be ON if the LAN connection is using 100BaseT, and Blinking if data is being transferred via the corresponding LAN port.• 10 LNK/ACT - This will be ON if the LAN connection is using 10BaseT, and Blinking if data is being transferred via the corresponding LAN port.• If neither LED is on, there is no active connection on the corresponding LAN port.
WLAN LED (ADW-4300 only)	On - Wireless enabled. Off - No Wireless connections currently exist. Flashing - Data is being transmitted or received via the Wireless access point. This includes "network traffic" as well as user data.
ADSL LED	On - ADSL connection is available. Off - No ADSL connection available. Flashing - Data is being transmitted or received via the ADSL connection.

Rear Panel

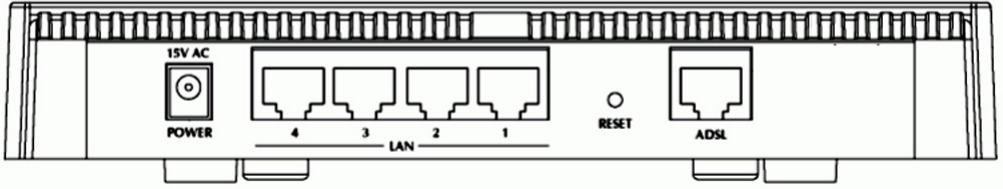


Figure 4: Rear Panel of ADE-4300

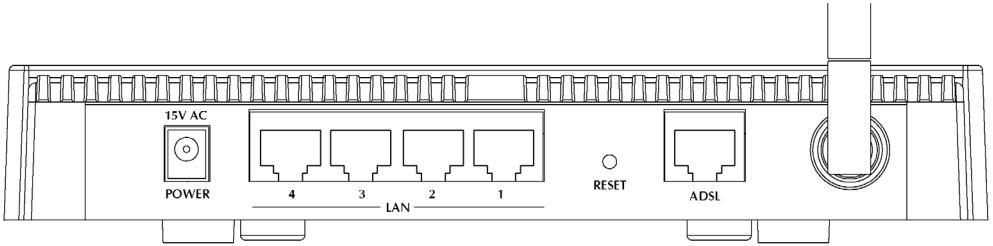


Figure 5: Rear Panel of ADW-4300

**RESET Button
(Reset to De-
faults)**

This button will reset the ADE-4300/ADW-4300 to the factory default settings.
To do this, press and hold the Reset Button for five (5) seconds, until the Status LED is lit, then release the Reset Button, and wait the ADE-4300/ADW-4300 to restart using the factory default values.

POWER port

Connect the supplied power adapter here.

**10/100BaseT
LAN connec-
tions**

Use standard LAN cables (RJ45 connectors) to connect your PCs to these ports.

Note:

Any LAN port on the ADE-4300/ADW-4300 will automatically function as an "Uplink" port when required. Just connect any port to a normal port on the other hub, using a standard LAN cable.

ADSL port

Connect this port to your ADSL line.

Chapter 2

Installation

2

This Chapter covers the physical installation of the ADE-4300/ADW-4300.

Requirements

- Network cables. Use standard 10/100BaseT network (UTP) cables with RJ45 connectors.
- TCP/IP protocol must be installed on all PCs.
- For Internet Access, an Internet Access account with an ISP, and a DSL connection.
- To use the Wireless Access Point, all Wireless devices must be compliant with the IEEE 802.11g or IEEE 802.11b specifications. (ADW-4300 only)

Procedure

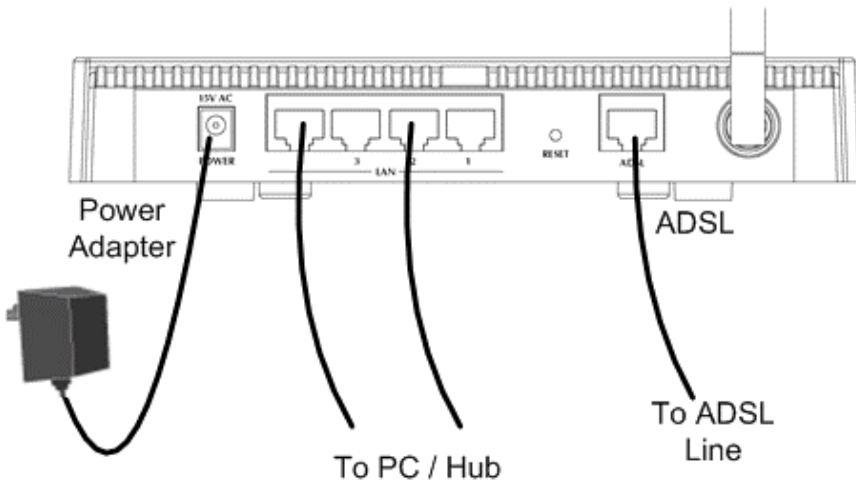


Figure 6: Installation Diagram (Antenna for ADW-4300 only)

1. Choose an Installation Site

Select a suitable place on the network to install the ADE-4300/ADW-4300.



For best Wireless reception and performance, the ADW-4300 should be positioned in a central location with minimum obstructions between the ADW-4300 and the PCs.

Also, if using multiple Access Points, adjacent Access Points should use different Channels.

2. Connect LAN Cables

Use standard LAN cables to connect PCs to the Switching Hub ports on the ADE-4300/ADW-4300. Both 10BaseT and 100BaseT connections can be used simultaneously.

If required, connect any port to a normal port on another Hub, using a standard LAN cable. Any LAN port on the ADE-4300/ADW-4300 will automatically function as an "Uplink" port when required.

3. Connect ADSL Cable

Connect the supplied ADSL cable from to the WAN port on the ADE-4300/ADW-4300 (the RJ11 connector) to the ADSL terminator provided by your phone company.

4. Power Up

Connect the supplied power adapter to the ADE-4300/ADW-4300. Use only the power adapter provided. Using a different one may cause hardware damage. Power it up by pressing the rear-mounted power switch.

5. Check the LEDs

- The *Power* LED should be ON.
- The *Status* LED should flash, then turn Off. If it stays on or blinking after 60 seconds, there is a hardware error.
- For each LAN (PC) connection, one of the LAN LEDs should be ON (provided the PC is also ON.)
- The *WLAN* LED should be ON. (ADW-4300 only)
- The *WAN* LED should be ON if ADSL line is connected.
- The *Internet* LED may be OFF. After configuration, it should come ON.

For more information, refer to *Front-mounted LEDs* in Chapter 1.

Chapter 3

Setup



This Chapter provides Setup details of the ADE-4300/ADW-4300.

Overview

This chapter describes the setup procedure for:

- Internet Access
- LAN configuration
- Wireless setup (ADW-4300 only)
- Assigning a Password to protect the configuration data.

PCs on your local LAN may also require configuration. For details, see *Chapter 4 - PC Configuration*.

Other configuration may also be required, depending on which features and functions of the ADE-4300/ADW-4300 you wish to use. Use the table below to locate detailed instructions for the required functions.

To Do this:	Refer to:
Configure PCs on your LAN.	Chapter 4: PC Configuration
Check ADE-4300/ADW-4300 operation and Status.	Chapter 5: Operation and Status
Use any of the following Advanced features: <ul style="list-style-type: none">• Internet (DMZ, Special Applications, URL Filter)• Dynamic DNS• Firewall Rules• Firewall Services• Schedule• Virtual Servers• VPN	Chapter 6: Advanced Features

<p>Use any of the following Administration Configuration settings or features:</p> <ul style="list-style-type: none">• PC Database• Config File• Logging• E-mail• Diagnostics• Remote Admin• Routing• Upgrade Firmware	<p>Chapter 7 Advanced Administration</p>
---	--

Configuration Program

The ADE-4300/ADW-4300 contains an HTTP server. This enables you to connect to it, and configure it, using your Web Browser. **Your Browser must support JavaScript.**

The configuration program has been tested on the following browsers:

- Netscape V4.08 or later
- Netscape 7
- Internet Explorer V5.01 or later

Preparation

Before attempting to configure the ADE-4300/ADW-4300, please ensure that:

- Your PC can establish a physical connection to the ADE-4300/ADW-4300. The PC and the ADE-4300/ADW-4300 must be directly connected (using the Hub ports on the ADE-4300/ADW-4300) or on the same LAN segment.
- The ADE-4300/ADW-4300 must be installed and powered ON.
- If the ADE-4300/ADW-4300's default IP Address (192.168.0.1) is already used by another device, the other device must be turned OFF until the ADE-4300/ADW-4300 is allocated a new IP Address during configuration.

Using your Web Browser

To establish a connection from your PC to the ADE-4300/ADW-4300:

1. After installing the ADE-4300/ADW-4300 in your LAN, start your PC. If your PC is already running, restart it.
2. Start your WEB browser.
3. In the *Address* box, enter "HTTP://" and the IP Address of the ADE-4300/ADW-4300, as in this example, which uses the ADE-4300/ADW-4300's default IP Address:

HTTP://192.168.0.1

4. When prompted for the User name and Password, enter default user name admin and leave the password field blank (no password).

If you can't connect

If the ADE-4300/ADW-4300 does not respond, check the following:

- The ADE-4300/ADW-4300 is properly installed, LAN connection is OK, and it is powered ON. You can test the connection by using the "Ping" command:
- Open the MS-DOS window or command prompt window.
- Enter the command:

```
ping 192.168.0.1
```

If no response is received, either the connection is not working, or your PC's IP address is not compatible with the ADE-4300/ADW-4300's IP Address. (See next item.)
- If your PC is using a fixed IP Address, its IP Address must be within the range 192.168.0.2 to 192.168.0.254 to be compatible with the ADE-4300/ADW-4300's default IP Address of 192.168.0.1. Also, the *Network Mask* must be set to 255.255.255.0. See *Chapter 4 - PC Configuration* for details on checking your PC's TCP/IP settings.
- Ensure that your PC and the ADE-4300/ADW-4300 are on the same network segment. (If you don't have a router, this must be the case.)
- Ensure you are using the wired LAN interface. The Wireless interface can only be used if its configuration matches your PC's wireless settings. (ADW-4300 only)

Setup Wizard

The first time you connect to the ADE-4300/ADW-4300, the Setup Wizard will run automatically. (The Setup Wizard will also run if the ADE-4300/ADW-4300's default settings are restored.)

1. Step through the Wizard until finished.
 - You need the data supplied by your ISP. Most connection methods require some data input.
 - The common connection types are explained in the following table.
2. On the final screen of the Wizard, run the test and check that an Internet connection can be established.
3. If the connection test fails:
 - Check all connections, and the front panel LEDs.
 - Check that you have entered all data correctly.

Common Connection Types

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	<p>a) ADSL parameters (VPI and VCI) may be required, if they cannot be detected automatically.</p> <p>b) Some ISP's may require you to use a particular <i>Host-name</i> or <i>Domain</i> name, or MAC (physical) address.</p>
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you. Usually, the connection is "Always on".	<p>a) ADSL parameters (VPI and VCI) may be required, if they cannot be detected automatically.</p> <p>b) IP Address allocated to you, and related information, such as Network Mask, Gateway IP address, and DNS address.</p>
PPPoE, PPPoA	You connect to the ISP only when required. The IP address is usually allocated automatically.	<p>a) ADSL parameters (VPI and VCI) may be required, if they cannot be detected automatically.</p> <p>b) User name and password are always required.</p> <p>c) If using a Static (Fixed) IP address, you need the IP address and related information (Network Mask, Gateway IP address, and DNS address)</p>
IPoA (IP over ATM)	Normally, the connection is "Always on".	<p>a) ADSL parameters (VPI and VCI) may be required, if they cannot be detected automatically.</p> <p>b) IP Address allocated to you, and related information, such as Network Mask, Gateway IP address, and DNS address.</p>

Home Screen

After finishing the Setup Wizard, you will see the *Home* screen. When you connect in future, you will see this screen when you connect. An example screen is shown below.

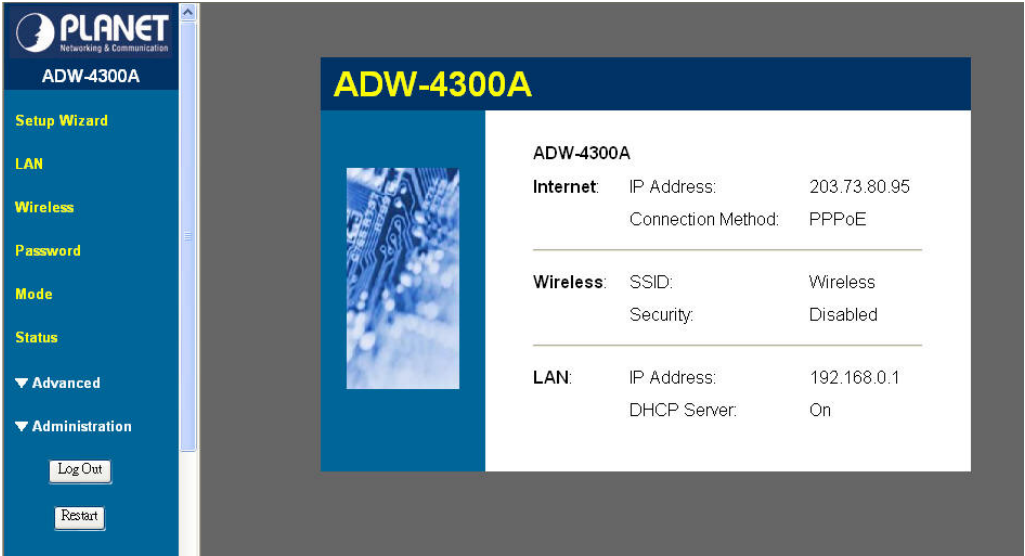


Figure 7: Home Screen

Main Menu

The main menu, on the left, contains links to the most-commonly used screen. To see the links to the other available screens, click "Advanced" or "Administration".

The main menu also contains two (2) buttons:

- **Log Out** - When finished, you should click this button to logout.
- **Restart** - Use this if you wish to restart the ADE-4300/ADW-4300. Note that restarting the Router will break any existing connections to or through the Router.

Navigation & Data Input

- Use the menu bar on the left of the screen, and the "Back" button on your Browser, for navigation.
- Changing to another screen without clicking "Save" does NOT save any changes you may have made. You must "Save" before changing screens or your data will be ignored.



On each screen, clicking the "Help" button will display help for that screen.

LAN Screen

Use the *LAN* link on the main menu to reach the LAN screen. An example screen is shown below.

Figure 8: LAN Screen

Data - LAN Screen

TCP/IP	
IP Address	IP address for the ADE-4300/ADW-4300, as seen from the local LAN. Use the default value unless the address is already in use or your LAN is using a different IP address range. In the latter case, enter an unused IP Address from within the range used by your LAN.
Subnet Mask	The default value 255.255.255.0 is standard for small (class "C") networks. For other networks, use the Subnet Mask for the LAN segment to which the ADE-4300/ADW-4300 is attached (the same value as the PCs on that LAN segment).
DHCP Server	<ul style="list-style-type: none"> If Enabled, the ADE-4300/ADW-4300 will allocate IP Addresses to PCs (DHCP clients) on your LAN when they start up. The default (and recommended) value is Enabled. If you are already using a DHCP Server, this setting must be Disabled, and the existing DHCP server must be re-configured to treat the ADE-4300/ADW-4300 as the default Gateway. See the following section for further details. The Start IP Address and Finish IP Address fields set the values used by the DHCP server when allocating IP Addresses to DHCP clients. This range also determines the number of DHCP clients supported. <p>See the following section for further details on using DHCP.</p>

DHCP

What DHCP Does

A DHCP (Dynamic Host Configuration Protocol) **Server** allocates a valid IP address to a DHCP **Client** (PC or device) upon request.

- The client request is made when the client device starts up (boots).

- The DHCP Server provides the *Gateway* and *DNS* addresses to the client, as well as allocating an IP Address.
- The ADE-4300/ADW-4300 can act as a **DHCP server**.
- Windows 95/98/ME and other non-Server versions of Windows will act as a DHCP **client**. This is the default Windows setting for the TCP/IP network protocol. However, Windows uses the term *Obtain an IP Address automatically* instead of "DHCP Client".
- You must NOT have two (2) or more DHCP Servers on the same LAN segment. (If your LAN does not have other Routers, this means there must only be one (1) DHCP Server on your LAN.)

Using the ADE-4300/ADW-4300's DHCP Server

This is the default setting. The DHCP Server settings are on the **LAN** screen. On this screen, you can:

- Enable or Disable the ADE-4300/ADW-4300's *DHCP Server* function.
- Set the range of IP Addresses allocated to PCs by the DHCP Server function.



You can assign Fixed IP Addresses to some devices while using DHCP, provided that the Fixed IP Addresses are NOT within the range used by the DHCP Server.

Using another DHCP Server

You can only use one (1) DHCP Server per LAN segment. If you wish to use another DHCP Server, rather than the ADE-4300/ADW-4300's, the following procedure is required.

- Disable the DHCP Server feature in the ADE-4300/ADW-4300. This setting is on the LAN screen.
- Configure the DHCP Server to provide the ADE-4300/ADW-4300's IP Address as the *Default Gateway*.

To Configure your PCs to use DHCP

This is the default setting for TCP/IP for all non-Server versions of Windows.

See *Chapter 4 - Client Configuration* for the procedure to check these settings.

Wireless Screen (ADW-4300 only)

The ADW-4300's settings must match the other Wireless stations.

Note that the ADW-4300 will automatically accept both 802.11b and 802.11g connections, and no configuration is required for this feature.

To change the ADW-4300's default settings for the Wireless Access Point feature, use the *Wireless* link on the main menu to reach the **Wireless** screen. An example screen is shown below.

Wireless

Identification

Region: Europe

Station Name: ADW-4300A

SSID (Service Set Identifier): Wireless

Options

802.11 Mode: 802.11g & 802.11b

Channel No: 11

☒ Broadcast SSID

Wireless Security

Current Setting: Disabled

Access Point

☒ Enable Wireless Access Point

Allow access by:

☒ ALL Wireless stations

☐ Trusted Wireless stations only

Configure

Set Stations

Save Cancel Help

Figure 9: Wireless Screen

Data - Wireless Screen

Identification	
Region	Select the correct domain for your location. It is your responsibility to ensure: <ul style="list-style-type: none">• That the ADW-4300 is only used in domains for which is licensed.• That you select the correct domain, so that only the legal channels for that domain can be selected.
Station name	This is the same as the "Device Name" for the ADW-4300.
SSID	This is also called the "Network Name". <ul style="list-style-type: none">• If using an ESS (Extended Service Set, with multiple access points) this ID is called an ESSID (Extended Service Set Identifier).• To communicate, all Wireless stations should use the same SSID/ESSID.

Options	
Mode	<p>Select the desired mode:</p> <ul style="list-style-type: none"> • 802.11G-plus (TI) This allows clients to use any of the following modes: <ul style="list-style-type: none"> • Standard 802.11b • 802.11B+ (Texas Instruments proprietary enhanced mode) • Standard 802.11g • 802.11G-plus (Texas Instruments proprietary enhanced mode). This mode can increase throughput by up to 50%, but will only work between compatible TI wireless stations. • 802.11g & 802.11b - Both 802.11.g and 802.11b Wireless stations will be able to use the ADW-4300. • 802.11g only - Only 802.11g Wireless stations can use the ADW-4300. • 802.11b only - Only 802.11b connections are available. 802.11g Wireless Stations will only be able to use the ADW-4300 if they are fully backward-compatible with the 802.11b standard.
Channel No.	<p>Select the Channel you wish to use on your Wireless LAN.</p> <ul style="list-style-type: none"> • If you experience interference (shown by lost connections and/or slow data transfers) you may need to experiment with different channels to see which is the best. • If using multiple Access Points, adjacent Access Points should use different Channels to reduce interference.
Broadcast SSID	<p>If enabled, the ADW-4300 will broadcast its SSID. This allows PCs and other wireless stations to detect this Access Point and use the correct SSID.</p> <p>If disabled, PC users will have to manually enter the SSID and other details of the wireless interface before they can connect to this Access Point.</p>
Wireless Security	
Current Setting	The current Wireless security is displayed. The default value is Disabled.
Configure Button	Click this button to access the Wireless security sub-screen, and view or change the settings. See the following section for details.
Access Point	
Enable Wireless Access Point	<p>Enable this if you want to use Wireless Access Point function.</p> <p>If disabled, no Wireless stations can use the Access Point function, and all connections must be made via the wired LAN.</p>

Allow access by ...	<p>Use this feature to determine which Wireless stations can use the Access Point. The options are:</p> <ul style="list-style-type: none">• All Wireless Stations - All wireless stations can use the access point, provided they have the correct SSID and security settings.• Trusted Wireless stations only - Only wireless stations you designate as "Trusted" can use the Access Point, even if they have the correct SSID and security settings. This feature uses the MAC address to identify Wireless stations. The MAC address is a low-level network identifier which is unique to each PC or network device. To define the trusted wireless stations, use the "Set Stations" button.
Set Stations Button	<p>Click this button to manage the trusted PC database.</p>

Wireless Security (ADW-4300 only)

This screen is accessed by clicking the "Configure" button on the *Wireless* screen. There are 3 options for Wireless security:

- **Disabled** - no data encryption is used.
- **WEP** - data is encrypted using the WEP standard.
- **WPA-PSK** - data is encrypted using the WPA-PSK standard. This is a later standard than WEP, and provides much better security than WEP. If all your Wireless stations support WPA-PSK, you should use WPA-PSK rather than WEP.

WEP Wireless Security

Wireless Security

Security System

WEP

Authentication Type:

Automatic

WEP Data Encryption:

128 bit (26 Hex chars)

Key 1:

☒ 87BF8014F2398A3487D7339485

Key 2:

☐

Key 3:

☐

Key 4:

☐

Passphrase:

Generate Keys

Save

Cancel

Help

Close

Figure 10: WEP

Data - WEP Screen

WEP Data Encryption	
WEP Data Encryption	<div>Select the desired option, and ensure the Wireless Stations use the same setting.</div> <ul style="list-style-type: none">• 64 Bit - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 64 Bit Encryption, the key size is 10 chars in HEX (0~9 and A~F).• 128 Bit - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 128 Bit Encryption, the key size is 26 chars in HEX (0~9 and A~F).
Authentication Type	Normally, this should be left at the default value of "Automatic". If changed to "Open System" or "Shared Key", ensure that your Wireless Stations use the same setting.
Default Key	Select the key you wish to be the default. Transmitted data is ALWAYS encrypted using the Default Key; the other Keys are for decryption only.

	You must enter a Key Value for the Default Key .
Key Value	Enter the key value or values you wish to use. The Default Key is required, the other keys are optional. Other stations must have the same key.
Passphrase	If desired, you can generate a key from a phrase, instead of entering the key value directly. Enter the desired phrase, and click the "Generate Keys" button.

WPA-PSK Wireless Security

Wireless Security

Security System

WPA-PSK

PSK :

Ab33kcjhIk54De8IEjly30vw

Encryption:

TKIP

Save

Cancel

Help

Close

Figure 11: WPA-PSK

Data - WPA-PSK Screen

Security System	WPA-PSK Like WEP, data is encrypted before transmission. WPA is more secure than WEP, and should be used if possible. WPA-PSK is the version of WPA, which does NOT require a Radius Server on your LAN.
PSK	Enter the PSK (network key). Data is encrypted using a key derived from the network key. Other Wireless Stations must use the same network key. The PSK must be from 8 to 63 characters in length.
WPA Encryption	The WPA-PSK standard allows different encryption methods to be used. Wireless Stations must use the same encryption method.

Trusted Wireless Stations (ADW-4300 only)

This feature can be used to prevent unknown Wireless stations from using the Access Point. This list has no effect unless the setting *Allow access by trusted stations only* is enabled.

To change the list of trusted wireless stations, use the *Modify List* button on the *Access Control* screen. You will see a screen like the sample below.

Trusted Wireless Stations

Other Wireless Stations

<<

>>

Edit

Name:

Address: (Physical/MAC address)

Add

Clear

Help

Close

Figure 12: Trusted Wireless Stations

Data - Trusted Wireless Stations

Trusted Wireless Stations	This lists any Wireless Stations which you have designated as "Trusted".
Other Wireless Stations	This list any Wireless Stations detected by the Access Point, which you have not designated as "Trusted".
Name	The name assigned to the Trusted Wireless Station. Use this when adding or editing a Trusted Station.
Address	The MAC (physical) address of the Trusted Wireless Station. Use this when adding or editing a Trusted Station.
Buttons	
<<	<div>Add a Trusted Wireless Station to the list (move from the "Other Stations" list).</div> <ul style="list-style-type: none">Select an entry (or entries) in the "Other Stations" list, and click the "<<" button.Enter the Address (MAC or physical address) of the wireless station, and click the "Add" button.
>>	<div>Delete a Trusted Wireless Station from the list (move to the "Other Stations" list).</div> <ul style="list-style-type: none">Select an entry (or entries) in the "Trusted Stations" list.Click the ">>" button.

Edit	<p>Use this to change an existing entry in the "Trusted Stations" list:</p> <ol style="list-style-type: none">1. Select the Station in the <i>Trusted Station</i> list.2. Click the <i>Edit</i> button. The address will be copied to the "Address" field, and the <i>Add</i> button will change to <i>Update</i>.3. Edit the address (MAC or physical address) as required.4. Click <i>Update</i> to save your changes.
Add (Update)	<p>To add a Trusted Station which is not in the "Other Wireless Stations" list, enter the required data and click this button.</p> <p>When editing an existing Wireless Station, this button will change from <i>Add</i> to <i>Update</i>.</p>
Clear	<p>Clear the <i>Name</i> and <i>Address</i> fields.</p>

Password Screen

The password screen allows you to assign a password to the ADE-4300/ADW-4300.

Password

Password

The password protects the configuration data.
Once set (recommended), you will be prompted for the password when you connect.

Old Password

New password:

Verify password:

Save

Cancel


Help

Figure 13: Password Screen

Old Password	Enter the existing password in this field.
New password	Enter the new password here.
Verify pass- word	Re-enter the new password here.

You will be prompted for the password when you connect, as shown below.

Enter Network Password



Please type your user name and password.

Site: 192.168.0.1

Realm: NeedPassword

User Name

Password

☐ Save this password in your password list

OK

Cancel

Figure 14: Password Dialog

- The "User Name" is always `admin`
- Enter the password for the ADE-4300/ADW-4300, as set on the *Password* screen above. The default password is blank.

Mode Screen

Use this screen to change the mode between Router mode and Modem (Bridge) mode.

Figure 15: Mode Screen

Select the desired option, and click "Save".

Router	Both the ADSL Modem and the Router features are operational. In this mode, this device can provide shared Internet Access to all your LAN users. Also, by default, it acts a DHCP Server, providing an IP address and related information to all Wireless (ADW-4300 only) and LAN users.
Modem	<p>Only the ADSL Modem component is operational.</p> <ul style="list-style-type: none"> • All Router features are disabled. This device is "transparent" - it does not perform any operations or make any changes to the network traffic passing through it. • You need to have a DHCP Server on your LAN to provide IP addresses to the Wireless clients using this Access Point (ADW-4300). • All traffic received on either the Wireless (ADW-4300) or LAN interface will be sent over the ADSL connection.

Notes:

- Generally, you should NOT use modem mode. Only select this mode if you are sure this is what you want.
- After changing the mode, this device will restart, which will take a few seconds. The menu will also change, depending on the mode you are in.
- The Wireless Access Point (ADW-4300 only) can function in either Router or Modem mode. But generally it is not a good idea to combine a Modem with an Access Point, because all data received from the wireless stations will be sent over the modem connection. (Since the modem is transparent, it does not examine the traffic to determine whether the traffic is for the LAN or the WAN.)
- For details on using Modem Mode, see Chapter 8.

Chapter 4

4

PC Configuration

This Chapter details the PC Configuration required on the local ("Internal") LAN.

Overview

For each PC, the following may need to be configured:

- TCP/IP network settings
- Internet Access configuration
- Wireless configuration (ADW-4300 only)

Windows Clients

This section describes how to configure Windows clients for Internet access via the ADE-4300/ADW-4300.

The first step is to check the PC's TCP/IP settings.

The ADE-4300/ADW-4300 uses the TCP/IP network protocol for all functions, so it is essential that the TCP/IP protocol be installed and configured on each PC.

TCP/IP Settings - Overview

If using the default ADE-4300/ADW-4300's settings, and the default Windows TCP/IP settings, no changes need to be made.

- By default, the ADE-4300/ADW-4300 will act as a DHCP Server, automatically providing a suitable IP Address (and related information) to each PC when the PC boots.
- For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client.

If using a Fixed (specified) IP address, the following changes are required:

- The *Gateway* must be set to the IP address of the ADE-4300/ADW-4300
- The *DNS* should be set to the address provided by your ISP.



If your LAN has a Router, the LAN Administrator must re-configure the Router itself. Refer to *Chapter 8 - Advanced Setup* for details.

Checking TCP/IP Settings - Windows 9x/ME:

5. Select *Control Panel - Network*. You should see a screen like the following:

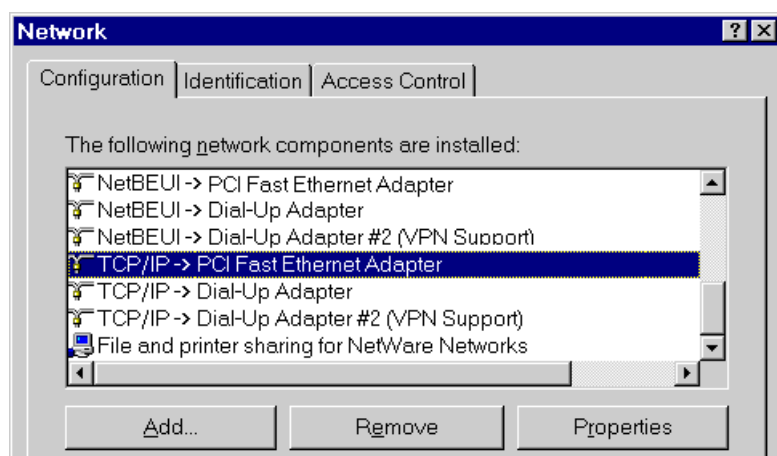


Figure 16: Network Configuration

6. Select the *TCP/IP* protocol for your network card.
7. Click on the *Properties* button. You should then see a screen like the following.

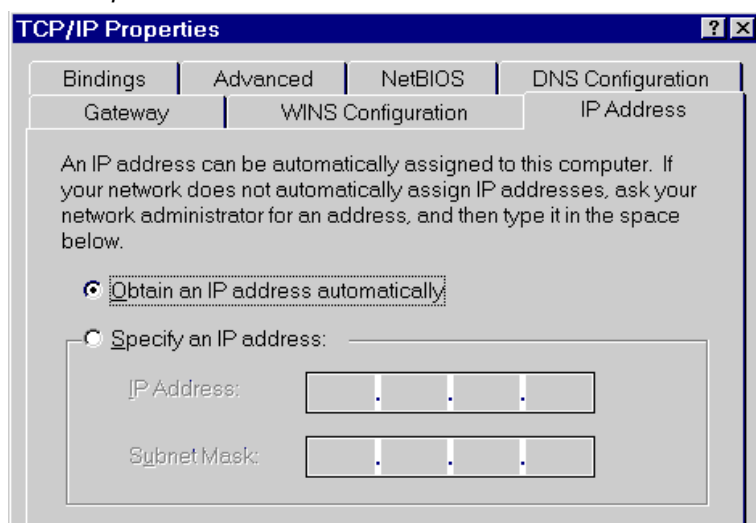


Figure 17: IP Address (Win 95)

Ensure your TCP/IP settings are correct, as follows:

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. **Using this is recommended.** By default, the ADE-4300/ADW-4300 will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the ADE-4300/ADW-4300.

Using "Specify an IP Address"

If your PC is already configured, check with your network administrator before making the following changes:

- On the *Gateway* tab, enter the ADE-4300/ADW-4300's IP address in the *New Gateway* field and click *Add*, as shown below. Your LAN administrator can advise you of the IP Address they assigned to the ADE-4300/ADW-4300.

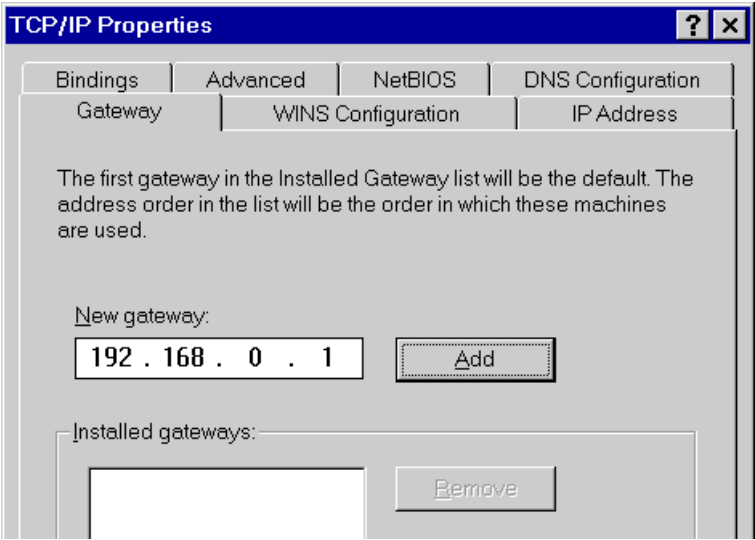


Figure 18: Gateway Tab (Win 95/98)

- On the *DNS Configuration* tab, ensure *Enable DNS* is selected. If the *DNS Server Search Order* list is empty, enter the DNS address provided by your ISP in the fields beside the *Add* button, then click *Add*.

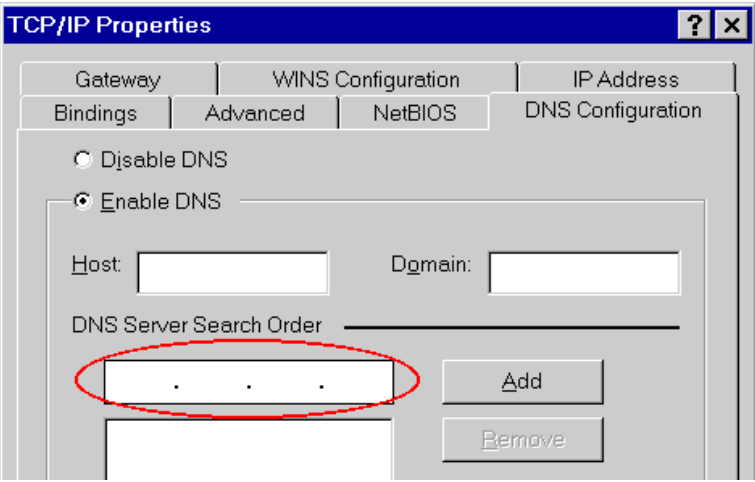


Figure 19: DNS Tab (Win 95/98)

Checking TCP/IP Settings - Windows NT4.0

1. Select *Control Panel - Network*, and, on the *Protocols* tab, select the TCP/IP protocol, as shown below.

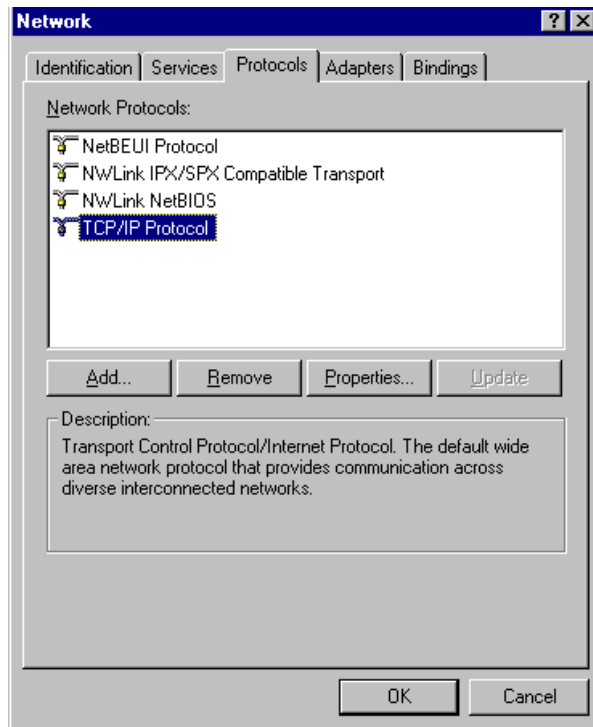


Figure 20: Windows NT4.0 - TCP/IP

2. Click the *Properties* button to see a screen like the one below.

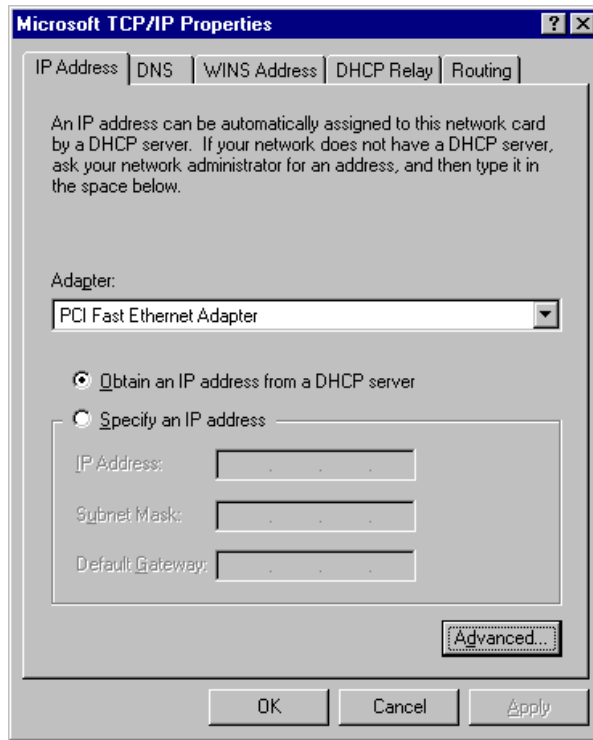


Figure 21: Windows NT4.0 - IP Address

3. Select the network card for your LAN.
4. Select the appropriate radio button - *Obtain an IP address from a DHCP Server* or *Specify an IP Address*, as explained below.

Obtain an IP address from a DHCP Server

This is the default Windows setting. **Using this is recommended.** By default, the ADE-4300/ADW-4300 will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the ADE-4300/ADW-4300.

Specify an IP Address

If your PC is already configured, check with your network administrator before making the following changes.

1. The *Default Gateway* must be set to the IP address of the ADE-4300/ADW-4300. To set this:
 - Click the *Advanced* button on the screen above.
 - On the following screen, click the *Add* button in the *Gateways* panel, and enter the ADE-4300/ADW-4300's IP address, as shown in Figure 22 below.
 - If necessary, use the *Up* button to make the ADE-4300/ADW-4300 the first entry in the *Gateways* list.

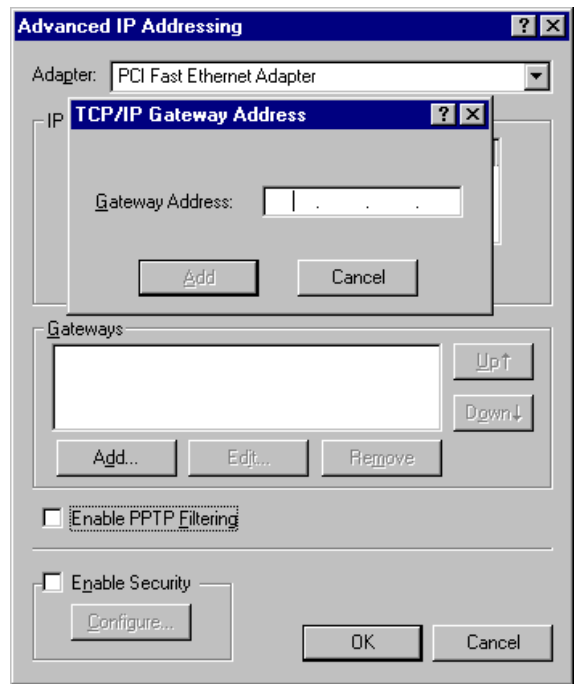


Figure 22 - Windows NT4.0 - Add Gateway

2. The DNS should be set to the address provided by your ISP, as follows:
- Click the DNS tab.
 - On the DNS screen, shown below, click the *Add* button (under *DNS Service Search Order*), and enter the DNS provided by your ISP.

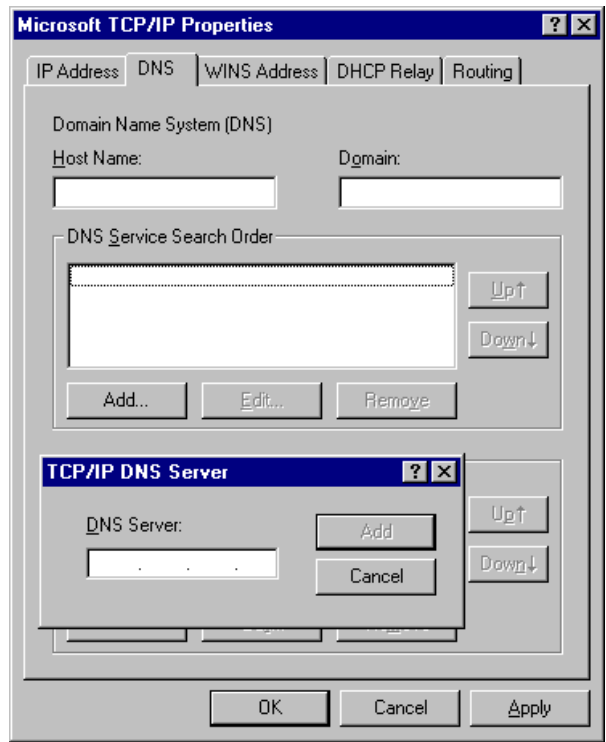


Figure 23: Windows NT4.0 - DNS

Checking TCP/IP Settings - Windows 2000:

1. Select *Control Panel - Network and Dial-up Connection*.
2. Right - click the *Local Area Connection* icon and select *Properties*. You should see a screen like the following:

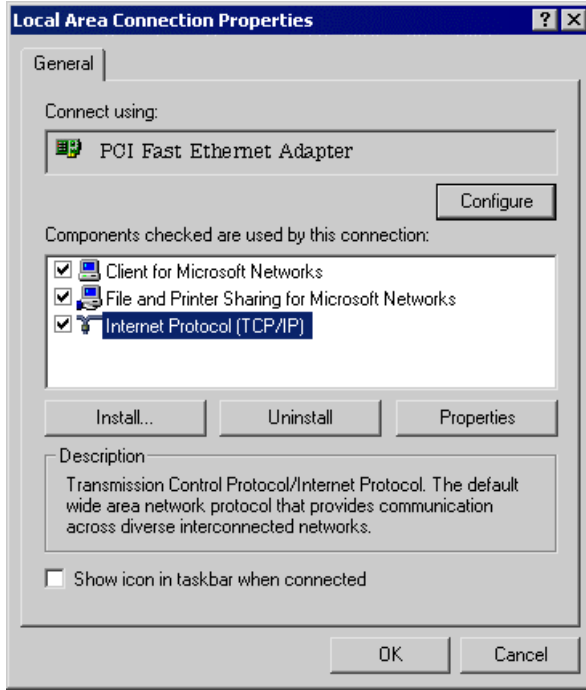


Figure 24: Network Configuration (Win 2000)

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.

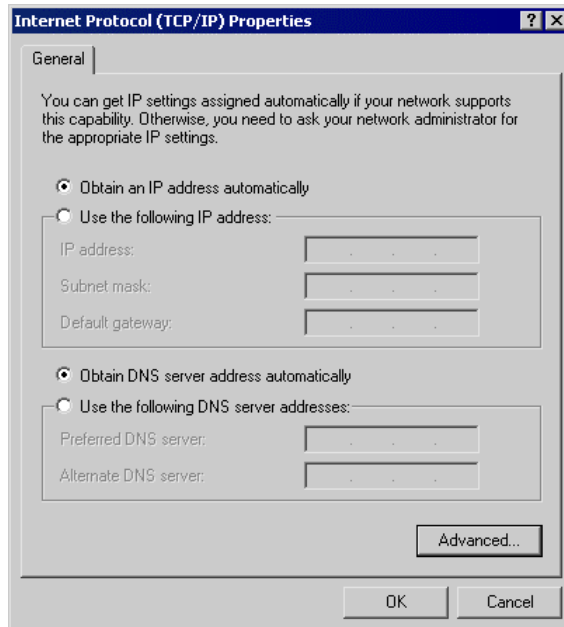


Figure 25: TCP/IP Properties (Win 2000)

5. Ensure your TCP/IP settings are correct, as described below.

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. **Using this is recommended.** By default, the ADE-4300/ADW-4300 will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the ADE-4300/ADW-4300.

Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes.

- Enter the ADE-4300/ADW-4300's IP address in the *Default gateway* field and click *OK*. (Your LAN administrator can advise you of the IP Address they assigned to the ADE-4300/ADW-4300.)
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the DNS address or addresses provided by your ISP, then click *OK*.

Checking TCP/IP Settings - Windows XP

1. Select *Control Panel - Network Connection*.
2. Right click the *Local Area Connection* and choose *Properties*. You should see a screen like the following:

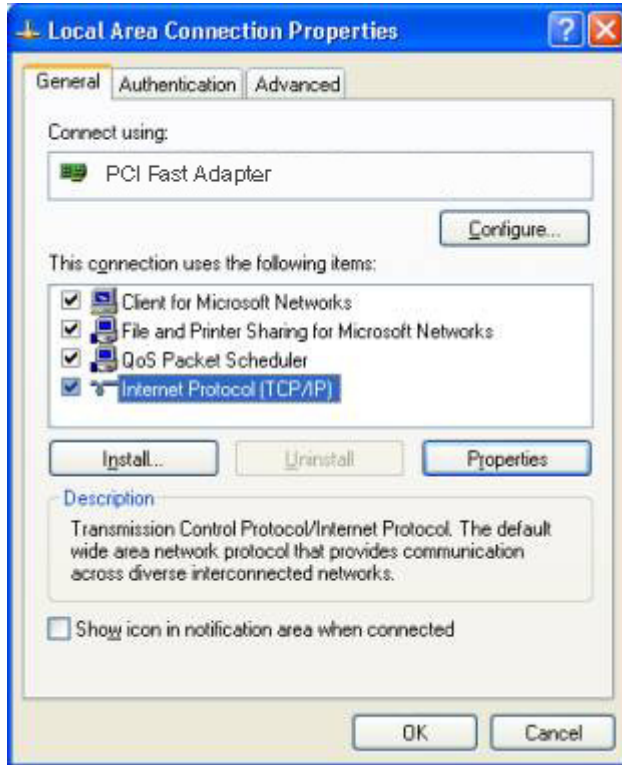


Figure 26: Network Configuration (Windows XP)

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.

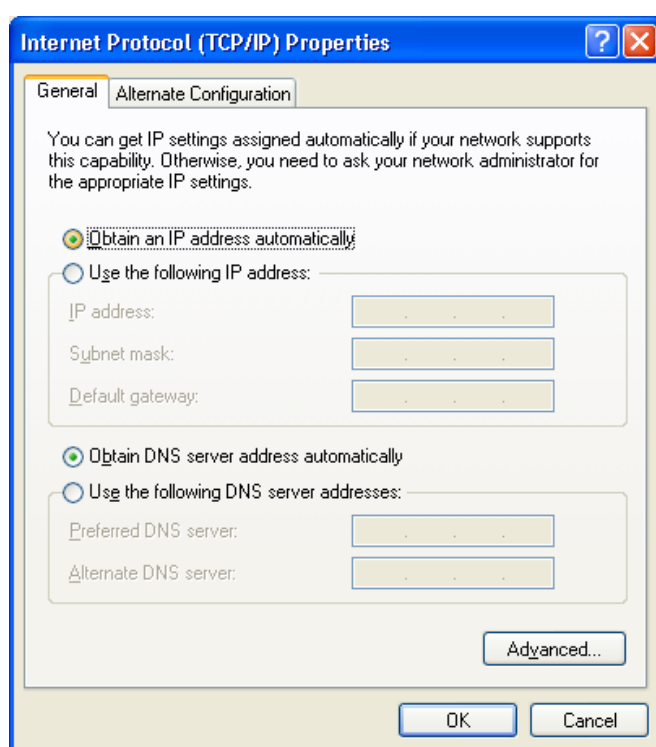


Figure 27: TCP/IP Properties (Windows XP)

5. Ensure your TCP/IP settings are correct.

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. **Using this is recommended.** By default, the ADE-4300/ADW-4300 will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the ADE-4300/ADW-4300.

Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes.

- In the *Default gateway* field, enter the ADE-4300/ADW-4300's IP address and click **OK**. Your LAN administrator can advise you of the IP Address they assigned to the ADE-4300/ADW-4300.
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the DNS address or addresses provided by your ISP, then click **OK**.

Internet Access

To configure your PCs to use the ADE-4300/ADW-4300 for Internet access:

- Ensure that the DSL modem, Cable modem, or other permanent connection is functional.
- Use the following procedure to configure your Browser to access the Internet via the LAN, rather than by a Dial-up connection.

For Windows 9x/ME/2000

1. Select *Start Menu - Settings - Control Panel - Internet Options*.
2. Select the *Connection* tab, and click the *Setup* button.
3. Select "I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)" and click *Next*.
4. Select "I connect through a local area network (LAN)" and click *Next*.
5. Ensure all of the boxes on the following Local area network Internet Configuration screen are **unchecked**.
6. Check the "No" option when prompted "Do you want to set up an Internet mail account now?".
7. Click *Finish* to close the Internet Connection Wizard.
Setup is now completed.

For Windows XP

1. Select *Start Menu - Control Panel - Network and Internet Connections*.
2. Select *Set up or change your Internet Connection*.
3. Select the *Connection* tab, and click the *Setup* button.
4. Cancel the pop-up "Location Information" screen.
5. Click *Next* on the "New Connection Wizard" screen.
6. Select "Connect to the Internet" and click *Next*.
7. Select "Set up my connection manually" and click *Next*.
8. Check "Connect using a broadband connection that is always on" and click *Next*.
9. Click *Finish* to close the New Connection Wizard.
Setup is now completed.

Accessing AOL

To access AOL (America On Line) through the ADE-4300/ADW-4300, the *AOL for Windows* software must be configured to use TCP/IP network access, rather than a dial-up connection. The configuration process is as follows:

- Start the *AOL for Windows* communication software. Ensure that it is Version 2.5, 3.0 or later. This procedure will not work with earlier versions.
- Click the *Setup* button.
- Select *Create Location*, and change the location name from "New Locality" to "ADE-4300/ADW-4300".
- Click *Edit Location*. Select *TCP/IP* for the *Network* field. (Leave the *Phone Number* blank.)
- Click *Save*, then *OK*.
Configuration is now complete.
- Before clicking "Sign On", always ensure that you are using the "ADE-4300/ADW-4300" location.

Macintosh Clients

From your Macintosh, you can access the Internet via the ADE-4300/ADW-4300. The procedure is as follows.

1. Open the TCP/IP Control Panel.
2. Select *Ethernet* from the *Connect via* pop-up menu.
3. Select *Using DHCP Server* from the *Configure* pop-up menu. The DHCP Client ID field can be left blank.
4. Close the TCP/IP panel, saving your settings.

Note:

If using manually assigned IP addresses instead of DHCP, the required changes are:

- Set the *Router Address* field to the ADE-4300/ADW-4300's IP Address.
- Ensure your DNS settings are correct.

Linux Clients

To access the Internet via the ADE-4300/ADW-4300, it is only necessary to set the ADE-4300/ADW-4300 as the "Gateway".

Ensure you are logged in as "root" before attempting any changes.

Fixed IP Address

By default, most Unix installations use a fixed IP Address. If you wish to continue using a fixed IP Address, make the following changes to your configuration.

- Set your "Default Gateway" to the IP Address of the ADE-4300/ADW-4300.
- Ensure your DNS (Name server) settings are correct.

To act as a DHCP Client (recommended)

The procedure below may vary according to your version of Linux and X -windows shell.

1. Start your X Windows client.
2. Select *Control Panel - Network*
3. Select the "Interface" entry for your Network card. Normally, this will be called "eth0".
4. Click the *Edit* button, set the "protocol" to "DHCP", and save this data.
5. To apply your changes
 - Use the "Deactivate" and "Activate" buttons, if available.
 - OR, restart your system.

Other Unix Systems

To access the Internet via the ADE-4300/ADW-4300:

- Ensure the "Gateway" field for your network card is set to the IP Address of the ADE-4300/ADW-4300.
- Ensure your DNS (Name Server) settings are correct.

Wireless Station Configuration (ADW-4300 only)

This section applies to all Wireless stations wishing to use the ADW-4300's Access Point, regardless of the operating system which is used on the client.

To use the Wireless Access Point in the ADW-4300, each Wireless Station must have compatible settings, as follows:

Mode	The mode must be set to Infrastructure (rather than Ad-hoc) Access points only operate in Infrastructure mode.
SSID (ESSID)	This must match the value used on the ADW-4300. The default value is Wireless . Note! The SSID is case sensitive.
Wireless Security	By default, Wireless security on the ADW-4300 is disabled. <ul style="list-style-type: none">If Wireless security remains disabled on the ADW-4300, all stations must have wireless security disabled.If Wireless security is enabled on the Wireless Router (either WEP or WPA-PSK), each station must use the same settings as the ADW-4300.

Wireless Configuration on Windows XP (ADW-4300 only)

If using Windows XP to configure the Wireless interface on your PC, the configuration procedure is as follows:

1. Open the Network Connections folder. (*Start - Settings - Network Connections*).

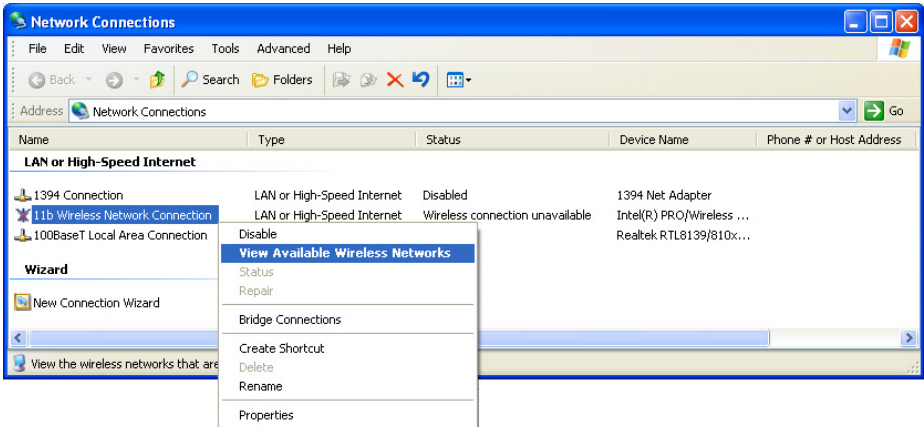


Figure 28: Network Connections (Windows XP)

2. Right-click the Wireless Network Connection, check that it is enabled (menu option says *Disable*, rather than *Enable*) and then select *View Available Wireless Networks*.
3. You will then see a list of wireless networks.

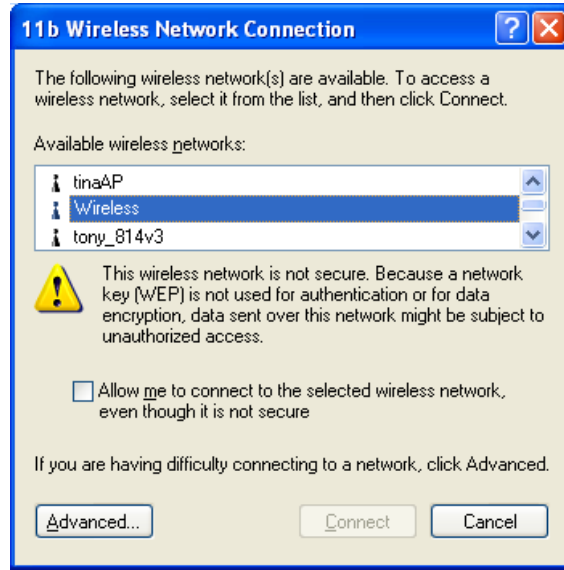


Figure 29 Wireless Networks (Windows XP)



If the "Broadcast SSID" setting on the ADW-4300 has been disabled, its SSID will NOT be listed. See the following section "If the SSID is not listed" for details of dealing with this situation.

4. The next step depends on whether or not Wireless security has been enabled on the ADW-4300.

If Wireless Security is Disabled

If Wireless security on the ADW-4300 is disabled, Windows will warn you that the Wireless network is not secure.

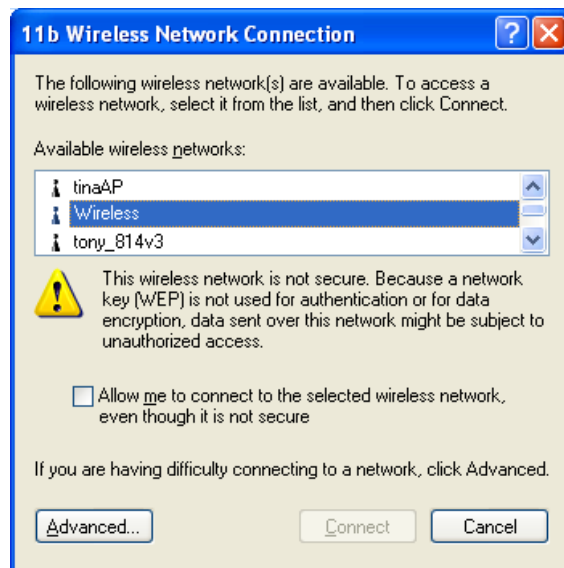


Figure 30 Insecure Wireless Network (Windows XP)

To connect:

- Check the checkbox *Allow me to connect to the selected wireless network, even though it is not secure*.
- The *Connect* button will then be available. Click the *Connect* button, and wait a few seconds for the connection to be established.

If using WEP Data Encryption

If WEP data encryption has been enabled on the ADW-4300, Windows will detect this, and show a screen like the following.

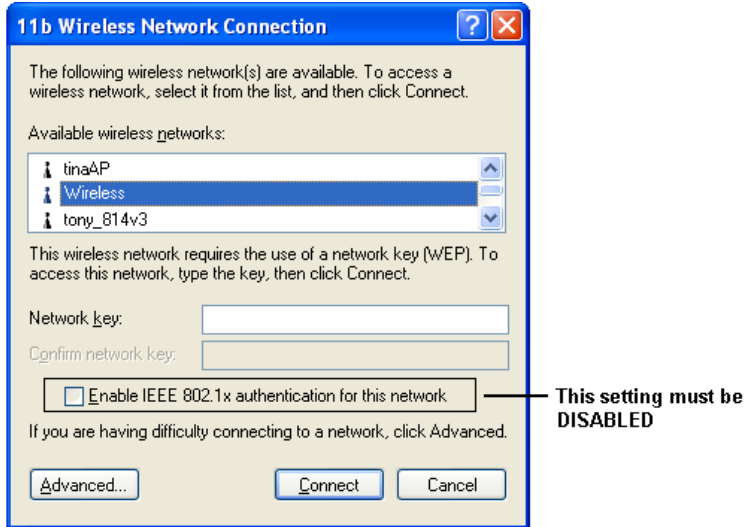


Figure 31: WEP (Windows XP)

To connect:

- Enter the WEP key, as set on the ADW-4300, in the *Network Key* field.
- Re-enter the WEP key into the *Confirm Network key* field.
- **Disable** the checkbox *Enable IEEE 802.1x authentication for this network*.
- Click the *Connect* button.

If this fails, click the *Advanced* button, to see a screen like the following:

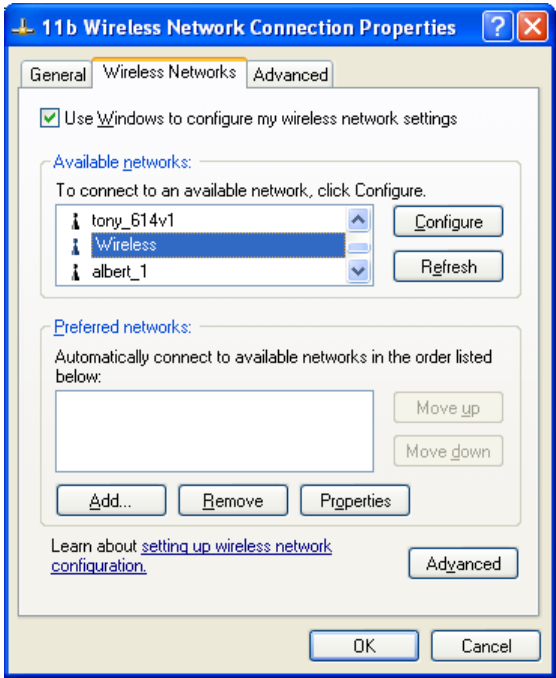


Figure 32: Advanced - Wireless Networks

Select the SSID for the ADW-4300, and click *Configure*, to see a screen like the following:

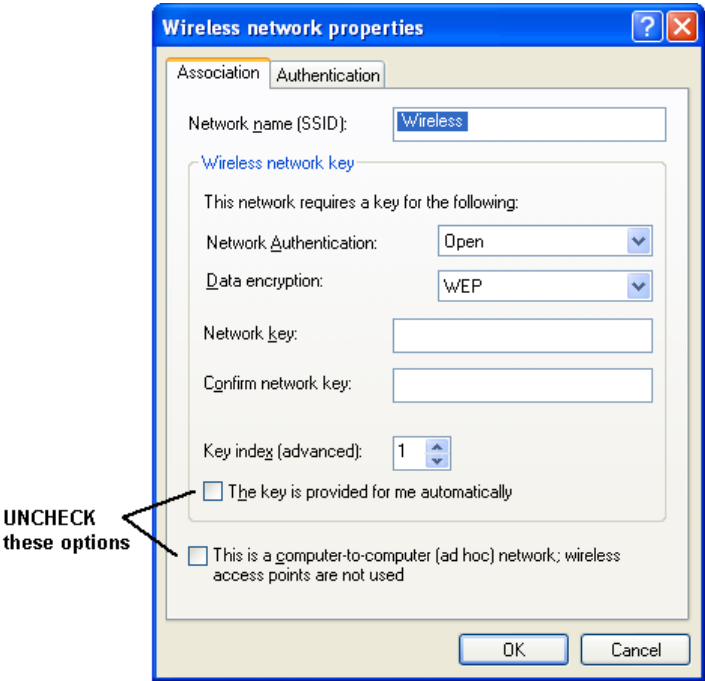


Figure 33: Wireless Network Properties - WEP

Configure this screen as follows:

- Set *Network Authentication* to match the ADW-4300. (If the setting on the ADW-4300 is "Auto", then either *Open* or *Shared* can be used.)
- For *Data Encryption*, select **WEP**.

- For the *Network key* and *Confirm network key*, enter the **default key value** used on the ADW-4300. (Windows will determine if 64bit or 128bit encryption is used.)
- The *Key index* must match the **default key index** on the ADW-4300. The default value is 1.
- Ensure the options *The key is provided for me automatically* and *This is a computer-to-computer (ad hoc) network* are unchecked.
- Click OK to save and close this dialog.
- This wireless network will now be listed in *Preferred Networks* on the screen below.

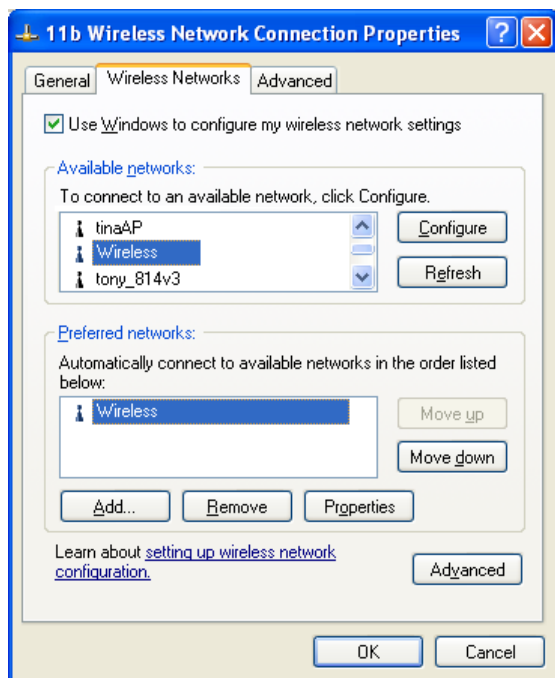


Figure 34: Preferred Networks

Click OK to establish a connection to the ADW-4300.

If using WPA-PSK Data Encryption

If WPA-PSK data encryption has been enabled on the ADW-4300, it does not matter which network is selected on the screen below. Just click the *Advanced* button.

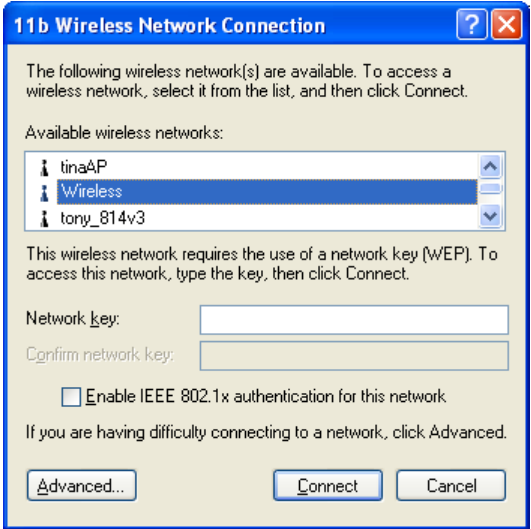


Figure 35: Wireless Networks (Windows XP)

You will then see a screen like the example below.

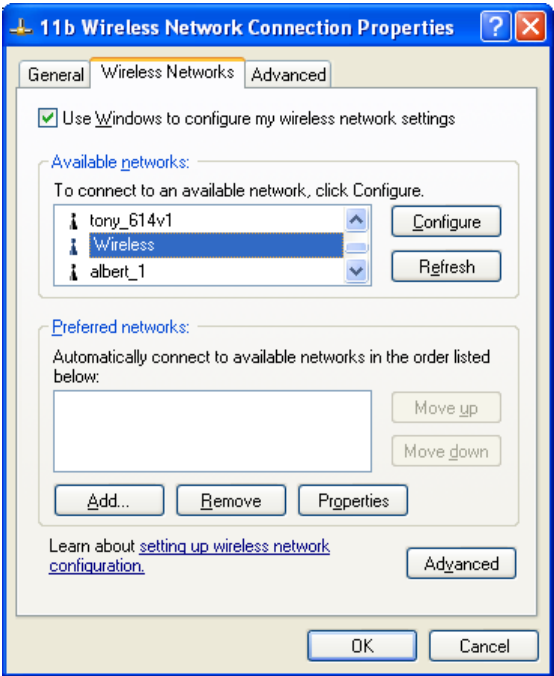


Figure 36: Advanced - Wireless Networks

Select the SSID for the ADW-4300, and click *Configure*, to see a screen like the following:

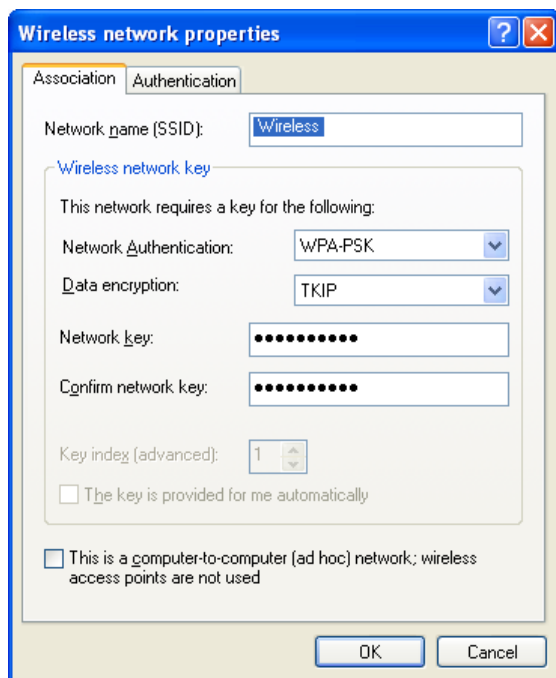


Figure 37: Wireless Network Properties- WPA-PSK

Configure this screen as follows:

- Set *Network Authentication* to **WPA-PSK**.
- For *Data Encryption*, select **TKIP**.
- For the *Network key* and *Confirm network key*, enter the network key (PSK) used on the ADW-4300.
- Ensure the option *This is a computer-to-computer (ad hoc) network* is unchecked.
- Click OK to save and close this dialog.
- This wireless network will now be listed in *Preferred Networks* on the screen below.

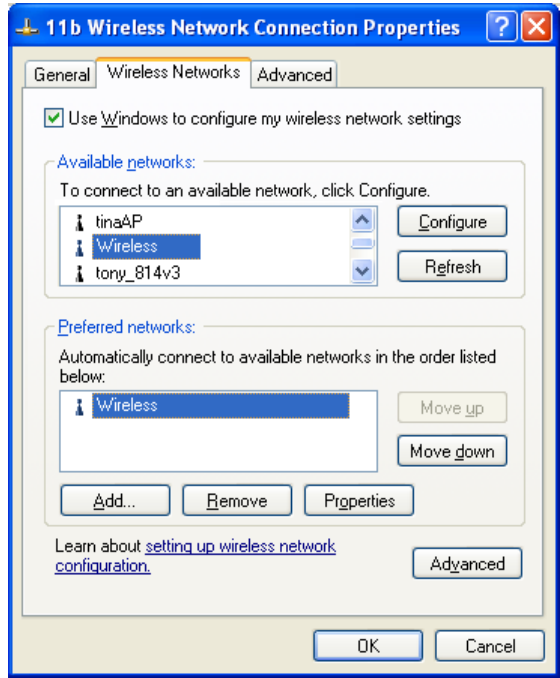


Figure 38: Preferred Networks

Click OK to establish a connection to the ADW-4300.

If the SSID is not listed

If the "Broadcast SSID" setting on the ADW-4300 has been disabled, its SSID will NOT be listed on the screen below.

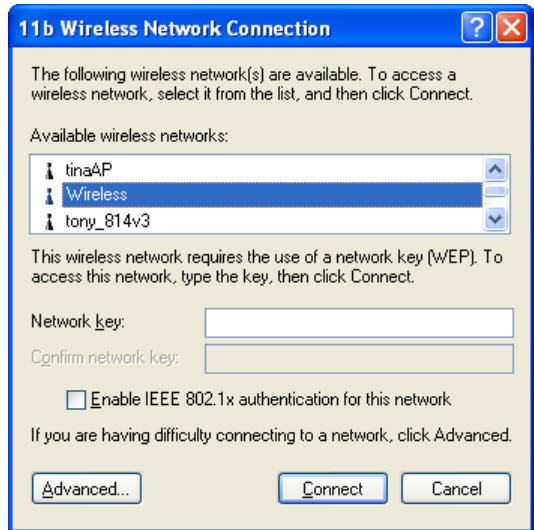


Figure 39: Wireless Networks (Windows XP)

In this situation, you need to obtain the SSID from your network administrator, then follow this procedure:

1. Click the *Advanced* button to see a screen like the example below.

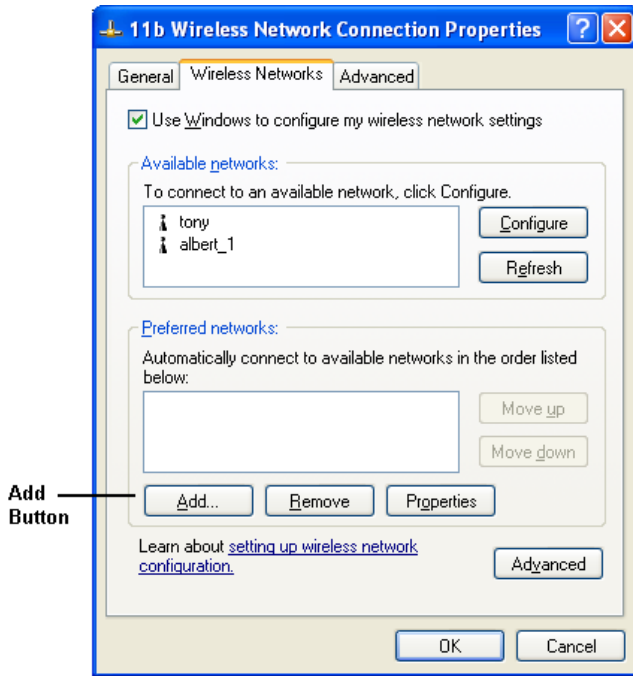


Figure 40: Unlisted Wireless Network

2. Click the *Add* button. You will see a screen like the example below.

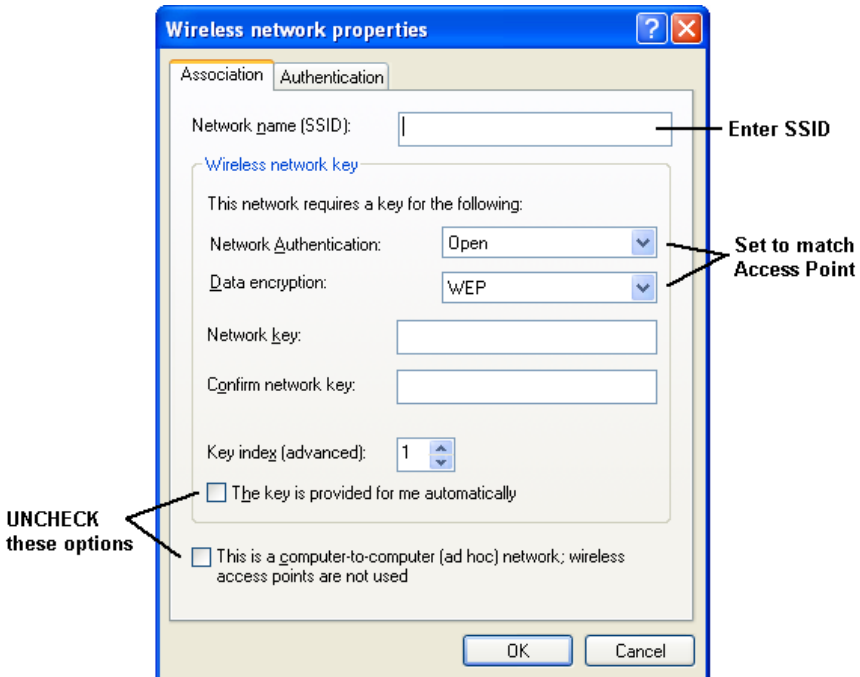


Figure 41: Add Wireless Network

3. Configure this screen as follows:
 - Enter the correct SSID, as used on the ADW-4300. Remember the SSID is case-sensitive, so be sure to match the case, not just the spelling.
 - Set *Network Authentication* and *Data Encryption* to match the ADW-4300.

- If using data encryption (WEP or WPA-PSK), enter the key used on the ADW-4300. See the preceding sections for details of WEP and WPA-PSK.
 - Uncheck the options *The key is provided for me automatically* and *This is a computer-to-computer (ad hoc) network*.
 - Click OK to save and exit.
4. This wireless network will then be listed in *Preferred Networks* on the screen below.

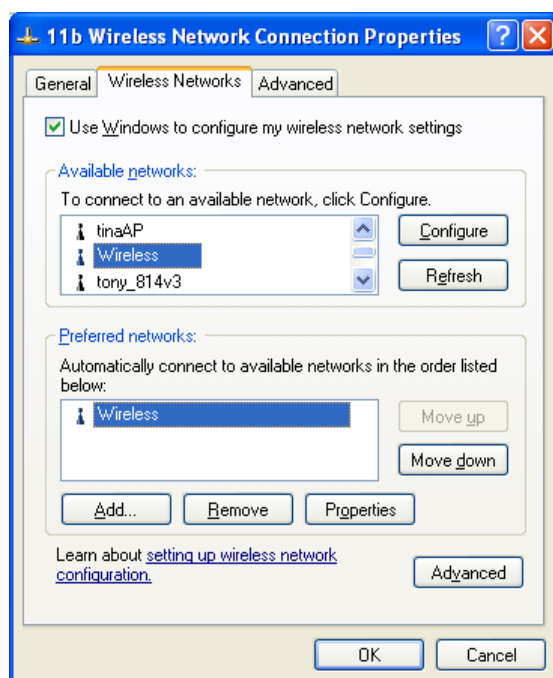


Figure 42: Preferred Networks

5. Click OK to establish a connection to the ADW-4300.

Chapter 5



Operation and Status

This Chapter details the operation of the ADE-4300/ADW-4300 and the status screens. For Details of operation in Bridge (Modem) mode, see Chapter 8 - Modem Mode.

Operation - Router Mode

Once both the ADE-4300/ADW-4300 and the PCs are configured, operation is automatic.

However, there are some situations where additional Internet configuration may be required. Refer to *Chapter 6 - Advanced Features* for further details.

Status Screen

Use the **Status** link on the main menu to view this screen.

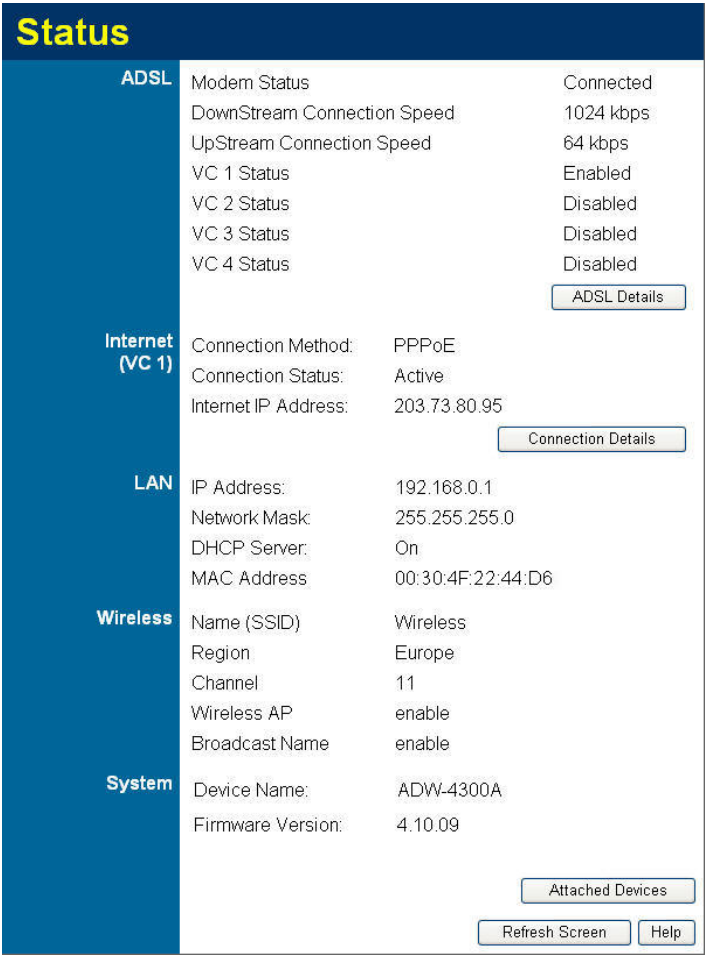


Figure 43: Status Screen

Data - Status Screen

ADSL	
Modem Status	This indicates the status of the ADSL modem component.
DownStream Connection Speed	Displays the speed for the DownStream Connection.
UpStream Connection Speed	If connected, displays the speed for the Up Stream (upload) ADSL Connection.
VC 1 Status VC 2 Status VC 3 Status VC 4 Status	For each VC (Virtual Circuit), the current status is displayed. This will be either "Enabled" or "Disabled". Note: VC 1 is a standard (Routed) Internet connection. VC 2, VC 3 and VC 4 are Bridge-mode connections.
Internet (VC1)	
Connection Method	Displays the current connection method, as set in the <i>Setup Wizard</i> .
Connection Status	This indicates the current status of the Internet Connection <ul style="list-style-type: none">Active - Connection exists

	<ul style="list-style-type: none"> • Idle - No current connection, but no error has been detected. This condition normally arises when an idle connection is automatically terminated. • Failed - The connection was terminated abnormally. This could be caused by Modem failure, or the loss of the connection to the ISP's server. <p>If there is an error, you can click the "Connection Details" button to find out more information.</p>
Internet IP Address	This IP Address is allocated by the ISP (Internet Service Provider). If using a dynamic IP address, and no connection currently exists, this information is unavailable.
LAN	
IP Address	The IP Address of the ADE-4300/ADW-4300.
Network Mask	The Network Mask (Subnet Mask) for the IP Address above.
DHCP Server	This shows the status of the DHCP Server function. The value will be "Enabled" or "Disabled".
MAC Address	This shows the MAC Address for the ADE-4300/ADW-4300, as seen on the LAN interface.
Wireless (ADW-4300 only)	
Name (SSID)	If using an ESS (Extended Service Set, with multiple access points) this ID is called an ESSID (Extended Service Set Identifier).
Region	The current region, as set on the Wireless screen.
Channel	This shows the Channel currently used, as set on the Wireless screen.
Wireless AP	This indicates whether or not the Wireless Access Point feature is enabled.
Broadcast Name	This indicates whether or not the SSID is Broadcast. This setting is on the Wireless screen.
System	
Device Name	The current name of the Router. This name is also the "hostname" for users with an "@Home" type connection.
Firmware Version	The version of the current firmware installed.
Buttons	
ADSL Details	Click this button to open a sub-window and view the details of each VC (Virtual Circuit).
Connection Details	Click this button to open a sub-window and view a detailed description of the current connection. Depending on the type of connection, a "log" may also be available.
Attached Devices	This will open a sub-window, showing all LAN and Wireless devices currently on the network.
Refresh Screen	Update the data displayed on screen.

Connection Status - PPPoE & PPPoA

If using PPPoE (PPP over Ethernet) or PPPoA (PPP over ATM), a screen like the following example will be displayed when the "Connection Details" button is clicked.

Connection Status

PPPoE / PPPoA

Connection Time00:18:02

Connection to ServerConnected

NegotiationSuccess

AuthenticationSuccess

IP Address203.73.80.95

Network Mask255.255.255.255

Connect

Disconnect

Close

Help

Figure 44: PPPoE Status Screen

Data - PPPoE/PPPoA Screen

Connection Time	This indicates how long the current connection has been established.
PPPoE Link Status	<div>This indicates whether or not the connection is currently established.<ul style="list-style-type: none">If the connection does not exist, the "Connect" button can be used to establish a connection.If the connection currently exists, the "Disconnect" button can be used to break the connection.</div>
Negotiation	This indicates the status of the PPPoE Server login.
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Network Mask	The Network Mask associated with the IP Address above.
Buttons	
Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, hang up the connection.
Close	Close this window.

Connection Details - Dynamic IP Address

If your access method is "Direct" (no login), with a Dynamic IP address, a screen like the following example will be displayed when the "Connection Details" button is clicked.

Connection Details	
Dynamic IP Address	
IP Address	172.31.2.205
Subnet Mask	255.255.255.0
Default Gateway	172.31.2.253
DNS Server	172.31.2.254
DHCP Server	172.31.2.205
Lease Obtained:	2002-09-08 12:06:02
Lease Expires:	2002-09-11 12:02:52
<input type="button" value="Release"/> <input type="button" value="Renew"/>	

Figure 45: Connection Details - Fixed/Dynamic IP Address

Data - Dynamic IP address

Internet	
IP Address	The current IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Network Mask	The Network Mask associated with the IP Address above.
Default Gateway	The IP address of the remote Gateway or Router associated with the IP Address above.
DHCP Server	The IP address of your ISP's DHCP Server.
DNS Server	The IP address of the Domain Name Server which is currently used.
Lease Obtained Lease Expires	This indicates when the current IP address was obtained, and how long before this IP address allocation (the DHCP lease) expires.
Buttons	
Release	If an IP Address has been allocated to the ADE-4300/ADW-4300 (by the ISP's DHCP Server, clicking the "Release" button will break the connection and release the IP Address.
Renew	If the ISP's DHCP Server has NOT allocated an IP Address for the ADE-4300/ADW-4300, clicking the "Renew" button will attempt to re-establish the connection and obtain an IP Address from the ISP's DHCP Server.
Close	Close this window.

Connection Details - Fixed IP Address

If your access method is "Direct" (no login), with a fixed IP address, a screen like the following example will be displayed when the "Connection Details" button is clicked.

Connection Status

Fixed IP Address

IP Address	172.31.2.205
Subnet Mask	255.255.255.0
Default Gateway	172.31.2.253
DNS Server	172.31.2.254

Close

Help

Figure 46: Connection Details - Fixed/Dynamic IP Address

Data - Fixed IP address Screen

Internet	
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Network Mask	The Network Mask associated with the IP Address above.
Default Gateway	The IP Address of the remote Gateway or Router associated with the IP Address above.
DNS Server	The IP Address of the Domain Name Server which is currently used.

Chapter 6

Advanced Features

This Chapter explains when and how to use the ADE-4300/ADW-4300's "Advanced" Features.

Overview

The following advanced features are provided:

- Access Control
 - Internet Access
 - Trusted PCs
- Internet:
 - DMZ
 - Special Applications
 - URL filter
- Dynamic DNS
- Firewall Rules
- Firewall Services
- Schedule
- Virtual Servers
- VPN
- SNMP

Access Control

The Access Control feature allows administrators to restrict the Internet Access available to PCs on your LAN by MAC address. With the default settings, everyone has unrestricted Internet access.

Access Control Screen

To view this screen, select the *Access Control* link on the Advanced menu.

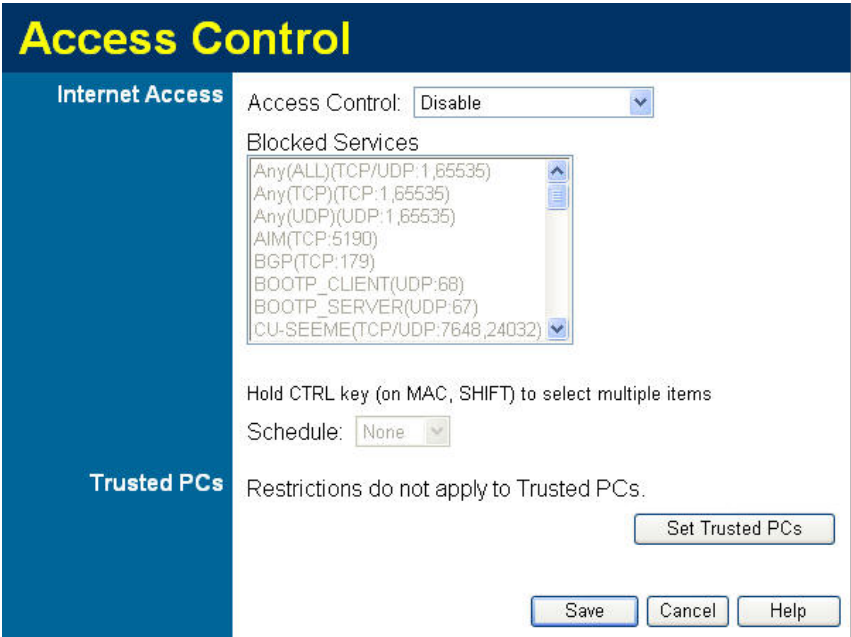


Figure 47: Access Control Screen

Data - Access Control Screen

Internet Access	
Access control	<p>Select the desired options for Internet access control:</p> <ul style="list-style-type: none">• Disable - Nothing is blocked.• Block all Internet access - All traffic via the WAN port is blocked.• Block selected Services - You can select which Services are to block. Hold CTRL key (on MAC, SHIFT) to select multiple items.
Schedule	<p>The administrator can choose Default Schedule to apply the blocking only during scheduled times. (If access is not blocked, no Scheduling is possible, and this setting has no effect.)</p> <ul style="list-style-type: none">• None - Schedule is disabled.• Default - Use the schedule which is defined in Schedule of Advanced Features.
Trusted PCs	
Set Trusted PCs	Restrictions do not apply to Trusted PCs.

Trusted PCs

This Trusted PC list has no effect unless the Internet Access feature is enabled. The list on the Trusted PCs will be bypassed from blockade of Internet access.

To change the list of trusted PCs, click the **Set Trusted PCs** button on the *Access Control* screen. You will see a screen like the sample below.

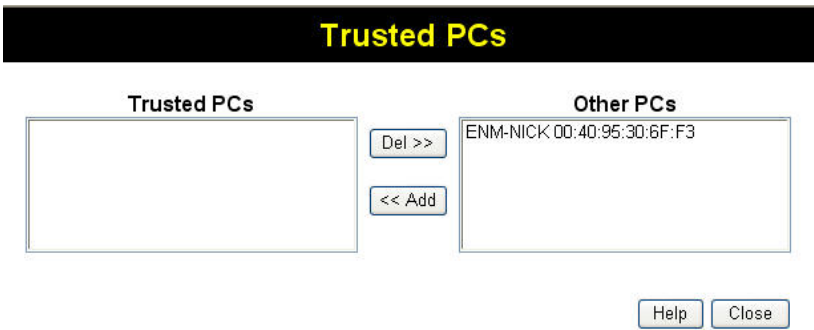


Figure 48: Trusted PCs

Data - Trusted PCs

Trusted PCs	
Trusted PCs	This lists any PCs which you have designated as “Trusted”.
Other PCs	This list any PCs detected by the router, which you have not designated as "Trusted".
Buttons	
<<	Add a Trusted PC to the list (move from the "Other PCs" list). <ul style="list-style-type: none">• Select an entry (or entries) in the "Other PCs" list, and click the " << " button.
>>	Delete a Trusted PC from the list (move to the "Other PCs" list). <ul style="list-style-type: none">• Select an entry (or entries) in the "Trusted PCs" list.• Click the " >> " button.

Note:

It is necessary to click the **Save** button in the Access Control page for activation of Trusted PCs if you add/delete any entry of Trusted PCs page.

Internet

This screen provides access to the DMZ, Special Applications and URL Filter features.

Figure 49: Internet Screen

DMZ

This feature, if enabled, allows the DMZ computer on your LAN to be exposed to all users on the Internet.

- This allows almost any application to be used on the "DMZ PC".
- The "DMZ PC" will receive all "Unknown" connections and data.
- If the DMZ feature is enabled, you must select the PC to be used as the "DMZ PC".



Note!

The "DMZ PC" is effectively outside the Firewall, making it more vulnerable to attacks. For this reason, you should only enable the DMZ feature when required.

Special Applications

If you use Internet applications which use non-standard connections or port numbers, you may find that they do not function correctly because they are blocked by the ADE-4300/ADW-4300. In this case, you can define the application as a "Special Application".

The **Special Applications** screen can be reached by clicking the *Special Applications* button on the *Internet* screen.

You can then define your Special Applications. You will need detailed information about the application; this is normally available from the supplier of the application.

Also, note that the terms "Incoming" and "Outgoing" on this screen refer to traffic from the client (PC) viewpoint

Special Applications

Enable	Name	Outgoing Ports			Incoming Ports		
		Type	Start	Finish	Type	Start	Finish
1. <input type="checkbox"/>		TCP			TCP		
2. <input type="checkbox"/>		TCP			TCP		
3. <input type="checkbox"/>		TCP			TCP		
4. <input type="checkbox"/>		TCP			TCP		
5. <input type="checkbox"/>		TCP			TCP		
6. <input type="checkbox"/>		TCP			TCP		
7. <input type="checkbox"/>		TCP			TCP		
8. <input type="checkbox"/>		TCP			TCP		
9. <input type="checkbox"/>		TCP			TCP		
10. <input type="checkbox"/>		TCP			TCP		
11. <input type="checkbox"/>		TCP			TCP		
12. <input type="checkbox"/>		TCP			TCP		

SaveCancel

HelpClose

Figure 50: Special Applications Screen

Data - Special Applications Screen

Checkbox	Use this to Enable or Disable this Special Application as required.
Name	Enter a descriptive name to identify this Special Application.
Incoming Ports	<ul style="list-style-type: none">Type - Select the protocol (TCP or UDP) used when you receive data from the special application or service. (Note: Some applications use different protocols for outgoing and incoming data).Start - Enter the beginning of the range of port numbers used by the application server, for data you receive. If the application uses a single port number, enter it in both the "Start" and "Finish" fields.Finish - Enter the end of the range of port numbers used by the application server, for data you receive.
Outgoing Ports	<ul style="list-style-type: none">Type - Select the protocol (TCP or UDP) used when you send data to the remote system or service.Start - Enter the beginning of the range of port numbers used by the application server, for data you send to it. If the application uses a single port number, enter it in both the "Start" and "Finish" fields.Finish - Enter the end of the range of port numbers used by the application server, for data you send to it. If the application uses a single port number, enter it in both the "Start" and "Finish" fields.

Using a Special Application

- Configure the *Special Applications* screen as required.
- On your PC, use the application normally. Remember that only one (1) PC can use each Special application at any time. Also, when 1 PC is finished using a particular Special Application, there may need to be a "Time-out" before another PC can use the same Special Application. The "Time-out" period may be up to 3 minutes.

URL Filter

If you want to limit access to certain sites on the Internet, you can use this feature. The URL filter will check each Web site access. If the address, or part of the address, is included in the block site list, access will be denied.

On the *Advanced Internet* screen, select the desired setting:

- **Disable** - disable this feature.
- **Block By Schedule** - block according to the settings on the *Schedule* page.
- **Block Always** - allow blocking all of the time, independent of the *Schedule* page.
- **Allow Trusted PCs to Visit Blocked Sites** - Enable this to allow specified computer(s) to have unrestricted access to the Internet. For this/these PC(s), the URL filter will be ignored.

To change the list of trusted PCs, click the **Set Trusted PCs** button on the *Access Control* screen. See Figure 46.

Data - Trusted PCs

Trusted PCs	
Trusted PCs	This lists any PCs which you have designated as "Trusted".
Other PCs	This list any PCs detected by the router, which you have not designated as "Trusted".
Buttons	
<<	Add a Trusted PC to the list (move from the "Other PCs" list). <ul style="list-style-type: none">• Select an entry (or entries) in the "Other PCs" list, and click the "<<" button.
>>	Delete a Trusted PC from the list (move to the "Other PCs" list). <ul style="list-style-type: none">• Select an entry (or entries) in the "Trusted PCs" list.• Click the ">>" button.

Click the **URL Filter List** button to open the URL Filter screen, allowing you to create or modify the filter strings which determine which sites will be blocked.

The **URL Filter List** screen is displayed when the **URL Filter List** button on the *Advanced Internet* screen is clicked.

Note:

It is necessary to click the **Save** button in the Access Control page for activation of Trusted PCs if you add/delete any entry of Trusted PCs page.

URL Filter List

When enabled, a request is blocked if any of these entries occur in the requested URL.

Current Filter Strings

Delete

Delete All

Add Filter String:

Add

Filter Strings should be as specific as possible.

Help

Close

Figure 51: URL Filter Screen

Data - URL Filter Screen

Current Filter Strings	
Current Filter Strings	<div>The list contains the current list of items to block.<ul style="list-style-type: none">To add to the list, use the "Add" option below.To delete an entry, select it and click Delete button.To delete all entries, click the Delete All button.</div>
Add Filter String	<div>To add to the current list, type the word or domain name you want to block into the field provided, then click the Add button.</div> <div>Filter strings should be as specific as possible. Otherwise, you may block access to many more sites than intended.</div>

63

Dynamic DNS (Domain Name Server)

This free service is very useful when combined with the *Virtual Server* feature. It allows Internet users to connect to your Virtual Servers using a URL, rather than an IP Address.

This also solves the problem of having a dynamic IP address. With a dynamic IP address, your IP address may change whenever you connect, which makes it difficult to connect to you.

DDNS Services work as follows:

1. You must register for the service at one of the listed DDNS Service providers.
2. After registration, use the Service provider's normal procedure to obtain your desired Domain name.
3. Enter your DDNS data on the ADE-4300/ADW-4300's DDNS screen, and enable the DDNS feature.
4. The ADE-4300/ADW-4300 will then automatically ensure that your current IP Address is recorded at the DDNS service provider's Domain Name Server.
5. From the Internet, users will be able to connect to your Virtual Servers (or DMZ PC) using your Domain name, as shown on this screen.

Dynamic DNS Screen

Select *Advanced* on the main menu, then *Dynamic DNS*, to see a screen like the following:

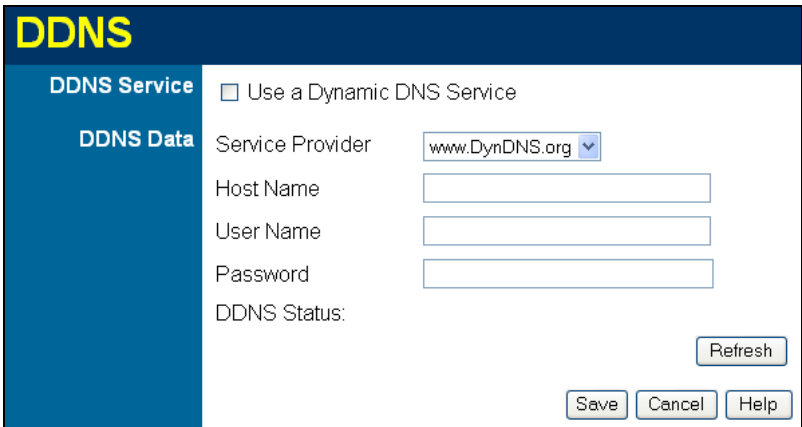


Figure 52: DDNS Screen

Data - Dynamic DNS Screen

DDNS Service	
Use a Dynamic DNS Service	Use this to enable or disable the DDNS feature as required.
Service Provider	Select the desired DDNS Service provider.
Web Site	Click this button to open a new window and connect to the Web site of the selected DDNS service provider.

DDNS Data	
Host Name	Enter the domain name allocated to you by the DDNS Service. If you have more than one name, enter the name you wish to use.
User Name	Enter your Username for the DDNS Service. (TZO.com uses your E-mail address.)
Password	Enter your current password for the DDNS Service. (TZO.com calls this a key.)
Domain Name	Enter the domain name allocated to you by the DDNS Service. If you have more than one name, enter the name you wish to use.
DDNS Status	<ul style="list-style-type: none">• This message is returned by the DDNS Server.• Normally, this message should be "Update successful"• If the message indicates some problem, you need to connect to the DDNS Service provider and correct this problem.

Firewall Rules

The **Firewall Rules** screen allows you to define "Firewall Rules" which can allow or prevent certain traffic. "Traffic" means incoming connection attempts, not packets.

By default:

- All Outgoing traffic is permitted.
- All Incoming traffic is denied.

Because of this default behavior, any **Outgoing** rules will generally **Block** traffic, and **Incoming** rules will generally **Allow** traffic.

Firewall Rules Screen

An example screen is shown below.

The screenshot shows a web interface titled "Firewall Rules". It contains two main sections: "Incoming Rules" and "Outgoing Rules". Each section has a table with columns: #, Enable, Service Name, Action, LAN Server IP address (for Incoming) or LAN Users (for Outgoing), WAN Users (for Incoming) or WAN Servers (for Outgoing), and Log. Below each table are buttons for "Add", "Edit", "Move", and "Delete". At the bottom right of the Outgoing Rules section are buttons for "Save", "Cancel", and "Help".

Incoming Rules							
#	Enable	Service Name	Action	LAN Server IP address	WAN Users	Log	
Default	Yes	Any	BLOCK always	--	Any	Match	

[Add](#) [Edit](#) [Move](#) [Delete](#)

Outgoing Rules							
#	Enable	Service Name	Action	LAN Users	WAN Servers	Log	
Default	Yes	Any	ALLOW always	Any	Any	Never	

[Add](#) [Edit](#) [Move](#) [Delete](#)

[Save](#) [Cancel](#) [Help](#)

Figure 53: Firewall Screen

Data - Firewall Rules

Incoming Rules	
#	For the default rule, this will display "Default". For rules which you create, this will display a radio button which allows you to select the rule.
Enable	Indicates whether or not the rule is currently enabled. For rules you have added, this column will contain a checkbox, allowing you to easily enable or disable the rule. (Click "Save" after making any changes.)
Service Name	The Service covered by this rule.
Action	The action performed on connections which are covered by this rule.
LAN Server	The PC or Server on your LAN to which traffic covered by this rule will be sent.

WAN Users	The WAN IP address or addresses covered by this rule.
Log	Indicates whether or not connections covered by this rule should be logged.
Buttons	Use the <i>Add</i> button to create a new rule. The other buttons - <i>Edit</i> , <i>Move</i> , or <i>Delete</i> - require that a rule be selected first. Use the radio buttons in the left column to select the desired rule.
Outgoing Rules	
#	For the default rule, this will display "Default". For rules which you create, this will display a radio button which allows you to select the rule.
Enable	Indicates whether or not the rule is currently enabled. For rules you have added, this column will contain a checkbox, allowing you to easily enable or disable the rule. (Click "Save" after making any changes.)
Service Name	The Service covered by this rule.
Action	The action performed on connections which are covered by this rule.
LAN Users	The LAN PC or PCs covered by this rule.
WAN Servers	The WAN IP address or addresses covered by this rule.
Log	Indicates whether or not connections covered by this rule should be logged.
Buttons	Use the <i>Add</i> button to create a new rule. The other buttons - <i>Edit</i> , <i>Move</i> , or <i>Delete</i> - require that a rule be selected first. Use the radio buttons in the left column to select the desired rule.

Incoming Rules (Inbound Services)

This screen is displayed when the "Add" or "Edit" button for Incoming Rules is clicked.

Inbound Services

Service:

Any(ALL)(TCP/UDP:1.65535)

Action:

ALLOW always

Send to LAN Server:

Select a PC

WAN Users:

Any

Single/Start:

Finish:

Log:

Always

Save

Cancel

Back

Help

Figure 54: Inbound Services Screen

Data - Incoming Rules Screen

Inbound Services	
Service	Select the desired Service. This determines which packets are covered by this rule. If necessary, you can define a new Service on the "Services" screen, by defining the protocols and port numbers used by the Service.
Action	<div>Select the desired action for packets covered by this rule:</div> <ul style="list-style-type: none">ALLOW alwaysALLOW by schedule, otherwise BlockBLOCK alwaysBLOCK by schedule, otherwise Allow <div>Note:</div> <ul style="list-style-type: none">Any inbound traffic which is not allowed by rules you create will be blocked by the Default rule.BLOCK rules are only useful if the traffic is already covered by an ALLOW rule. (That is, you wish to block a sub-set of traffic which is currently allowed by another rule.)To define the Schedule used in these selections, use the "Schedule" screen.
Send to LAN Server	Select the PC or Server on your LAN which will receive the inbound traffic covered by this rule.
WAN Users	<div>These settings determine which packets are covered by the rule, based on their source (WAN) IP address. Select the desired option:</div> <ul style="list-style-type: none">Any - All IP addresses are covered by this rule.Address range - If this option is selected, you must enter the

	<p>desired values in the "Single/Start" and "Finish" fields to determine the address range.</p> <ul style="list-style-type: none">• Single address - Enter the required address in the "Single/Start" fields.
Log	<p>This determines whether packets covered by this rule are logged. Select the desired action.</p> <ul style="list-style-type: none">• Always - always log traffic considered by this rule, whether it matches or not. (This is useful when debugging your rules.)• Never - never log traffic considered by this rule, whether it matches or not.• Match - Log traffic only it matches this rule. (The action is determined by this rule.)• Not Match - Log traffic which is considered by this rule, but does not match (The action is NOT determined by this rule.)

Outgoing Rules (Outbound Services)

This screen is displayed when the "Add" or "Edit" button for Outgoing Rules is clicked.

Outbound Services

Service

Any(ALL)(TCP/UDP:1,65535)

Action

BLOCK always

LAN Users

Any

PC:

Select a PC

WAN Users

Any

Single/Start:

Finish:

Log

Always

Save

Cancel

Back

Help

Figure 55: Outbound Services Screen

Data - Outbound Rules Screen

Outbound Services	
Service	Select the desired Service or application to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the "Services" menu option
Action	<p>Select the desired action for packets covered by this rule:</p> <ul style="list-style-type: none">• BLOCK always• BLOCK by schedule, otherwise Allow• ALLOW always

	<ul style="list-style-type: none"> • ALLOW by schedule, otherwise Block <p>Note:</p> <ul style="list-style-type: none"> • Any outbound traffic which is not blocked by rules you create will be allowed by the Default rule. • ALLOW rules are only useful if the traffic is already covered by a BLOCK rule. (That is, you wish to allow a subset of traffic which is currently blocked by another rule.) • To define the Schedule used in these selections, use the "Schedule" screen.
LAN Users	<p>Select the desired option to determine which PCs are covered by this rule:</p> <ul style="list-style-type: none"> • Any - All PCs are covered by this rule. • Single PC - Only the selected PC is covered by this rule. If selected, you must select the PC. <p>PC - If using Single PC above, select the PC or Server on your LAN which will be covered by this rule.</p>
WAN Users	<p>These settings determine which packets are covered by the rule, based on their source (WAN) IP address. Select the desired option:</p> <ul style="list-style-type: none"> • Any - All IP addresses are covered by this rule. • Address range - If this option is selected, you must enter the "Start" and "Finish" fields. • Single address - Enter the required address in the "Single/Start" fields.
Log	<p>This determines whether packets covered by this rule are logged. Select the desired action.</p> <ul style="list-style-type: none"> • Always - always log traffic considered by this rule, whether it matches or not. (This is useful when debugging your rules.) • Never - never log traffic considered by this rule, whether it matches or not. • Match - Log traffic only it matches this rule. (The action is determined by this rule.) • Not Match - Log traffic which is considered by this rule, but does not match (The action is NOT determined by this rule.)

Firewall Services

Services are used when creating Firewall Rules.

If you wish to create a firewall rule, but the required service is not listed in the "Service" list, you can use this feature to define the required service or services. Once created, these services will be listed in the "Service" list, and can be used when creating Firewall Rules.

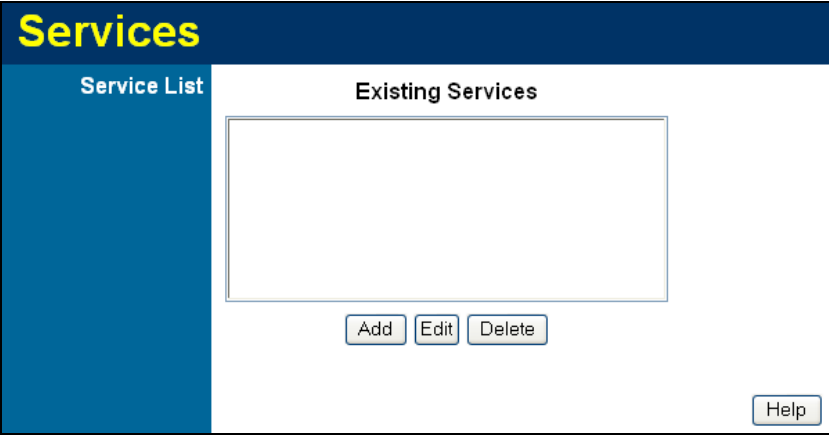


Figure 56: Add Services Screen

Data - Firewall Services

Services	
Existing Services	<p>This lists any Services you have defined. If you have not defined any Services, this list will be empty.</p> <p>Once you define some services, they will be listed here, and also shown in the Service list used to create Firewall rules. (Firewall services are at the end of the list, after the pre-defined services.)</p>
Add	<p>Use this to open a sub-screen where you can add a new service.</p>
Edit	<p>To modify a service, select it, and then click this button.</p>
Delete	<p>Use this button to delete the selected service. You can delete any services you have defined.</p>

Add/Edit Service

This screen is displayed when the *Add* or *Edit* button on the **Services** screen is clicked.

Add/Edit Service

Name:

Type:

TCP

Start Port:

Finish Port:

Figure 57 : Add/Edit Service

Data - Add/Edit Service

Services	
Name	If editing, this shows the current name of the Service. If adding a new service, this will be blank, and you should enter a suitable name.
Type	Select the protocol used by the Service.
Start Port	Enter the beginning of the port range used by the Service.
Finish Port	Enter the end of the port range used by the Service.

Options

This screen allows advanced users to enter or change a number of settings. For normal operation, there is no need to use this screen or change any settings.

An example **Options** screen is shown below.

The screenshot shows a web interface titled "Options" in yellow text on a dark blue header. Below the header is a sidebar with two main sections: "Internet" and "UPnP", both in white text on a blue background. The "Internet" section contains a checkbox labeled "Respond to Ping on Internet (WAN) Port" which is currently unchecked, and a text input field for "MTU Size" with the value "1492" and a note "(Bytes, 1~1500)". The "UPnP" section contains a checkbox labeled "Enable UPnP" which is checked, and two text input fields: "Advertisement Period" with the value "30" and note "(Minutes, 1~1440)", and "Advertisement Time to Live" with the value "4" and note "(Hops, 1~255)". At the bottom right of the form are three buttons: "Save", "Cancel", and "Help".

Figure 58: Options Screen

Data - Options Screen

Internet	
Respond to Ping	<ul style="list-style-type: none">• If checked, the Wireless Router will respond to Ping (ICMP) packets received from the Internet.• If not checked, Ping (ICMP) packets from the Internet will be ignored. Disabling this option provides a slight increase in security.
MTU Size	<p>Enter a value between 1 and 1500.</p> <p>Note: MTU (Maximum Transmission Unit) size should only be changed if advised to do so by Technical Support.</p>
UPnP	
UPnP	<ul style="list-style-type: none">• UPnP (Universal Plug and Play) allows automatic discovery and configuration of equipment attached to your LAN. UPnP is by supported Windows ME, XP, or later.• If Enabled, this device will be visible via UPnP.• If Disabled, this device will not be visible via UPnP.
Advertisement Period	<p>Enter the desired value, in minutes. The valid range is from 1 to 1440.</p>
Advertisement Time to Live	<p>Enter the desired value, in hops. The valid range is from 1 to 255.</p>

Schedule

This Schedule can be used for the Firewall Rules and the URL filter.

Schedule

Schedule

Use 24 hour clock. On all day: 00:00 to 24:00
Off all day: All fields blank

Day	Session 1		Session 2	
	Start	Finish	Start	Finish
Monday	00:00	12:00	12:00	24:00
Tuesday	00:00	12:00	12:00	24:00
Wednesday	00:00	12:00	12:00	24:00
Thursday	00:00	12:00	12:00	24:00
Friday	00:00	12:00	12:00	24:00
Saturday	00:00	12:00	12:00	24:00
Sunday	00:00	12:00	12:00	24:00

Local Time

Time Zone: (GMT) Greenwich Mean Time : Edinburgh, London

☐ Adjust for Daylight Savings Time

☐ Use this NTP Server . . .

Current Time: 2005-06-01 08:28:37

[Save](#) [Cancel](#) [Help](#)

Figure 59: Schedule Screen

Data - Schedule Screen

Schedule	
Day	Each day of the week can scheduled independently.
Session 1 Session 2	Two (2) separate sessions or periods can be defined. Session 2 can be left blank if not required.
Start Time	Enter the start using a 24 hr clock.
Finish Time	Enter the finish time using a 24 hr clock.
Local Time	
Time Zone	In order to display your local time correctly, you must select your "Time Zone" from the list.
Adjust for Day-light Savings Time	If your region uses Daylight Savings Time, you must manually check "Adjust for Daylight Savings Time" at the beginning of the adjustment period, and uncheck it at the end of the Day-light Savings period.

Use this NTP Server	<p>If you prefer to use a particular NTP server as the primary NTP server, check the checkbox "Use this NTP Server" and enter the Server's IP address in the fields provided..</p> <p>If this setting is not enabled, the default NTP Servers are used.</p>
Current Time	<p>This displays the current time on the ADE-4300/ADW-4300, at the time the page is loaded.</p>

Virtual Servers

This feature, sometimes called *Port Forwarding*, allows you to make Servers on your LAN accessible to Internet users. Normally, Internet users would not be able to access a server on your LAN because:

- Your Server does not have a valid external IP Address.
- Attempts to connect to devices on your LAN are blocked by the firewall in this device.

The "Virtual Server" feature solves these problems and allows Internet users to connect to your servers, as illustrated below.

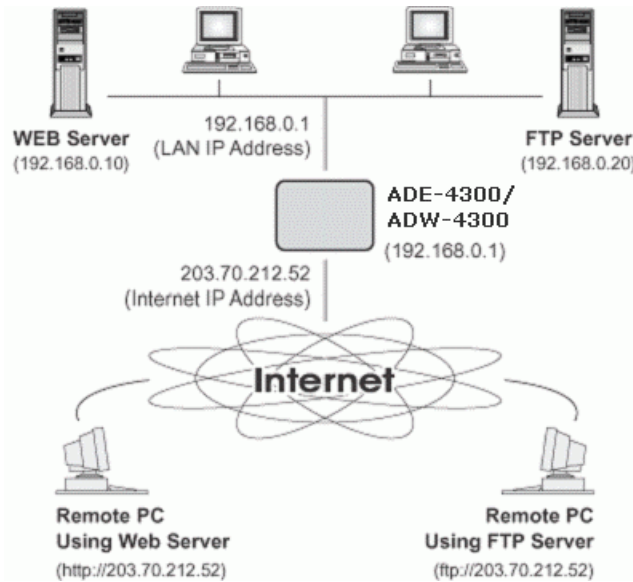


Figure 60: Virtual Servers

IP Address seen by Internet Users

Note that, in this illustration, both Internet users are connecting to the same IP Address, but using different protocols.

To Internet users, all virtual Servers on your LAN have the same IP Address. This IP Address is allocated by your ISP.

This address should be static, rather than dynamic, to make it easier for Internet users to connect to your Servers.

However, you can use the *DDNS (Dynamic DNS)* feature to allow users to connect to your Virtual Servers using a URL, instead of an IP Address.

Virtual Servers Screen

- The "Virtual Servers" feature allows Internet Users to access PCs on your LAN.
- The PCs must be running the appropriate Server Software.
- For Internet Users, ALL of your Servers have the same IP address. This IP address is allocated by your ISP.
- To make it easier for Internet users to connect to your Servers, you can use the "DDNS" feature. This allows Internet users to connect to your Servers with a URL, rather than an IP address. This technology works even if your ISP allocates dy-

dynamic IP addresses (IP address is allocated upon connection, so it may change each time you connect).

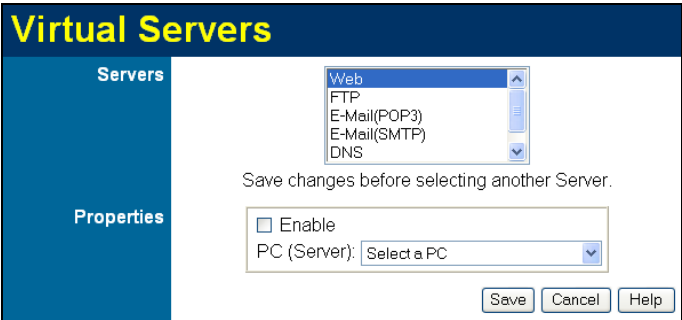


Figure 61: Virtual Servers Screen

Data - Virtual Servers Screen

Servers	
Servers	This lists a number of common Server types. If the desired Server type is not listed, you can create a Firewall Rule to achieve the same effect as the Virtual Server function.
Properties	
Enable	Use this to Enable or Disable support for this Server, as required. If Enabled, you must select the PC to which this traffic will be sent.
PC (Server)	Select the PC for this Server. The PC must be running the appropriate Server software.



Note!

For each entry, the PC must be running the appropriate Server software.

If the desired Server type is not listed, you can define your own Servers, using the Firewall Rules.

Connecting to the Virtual Servers

Once configured, anyone on the Internet can connect to your Virtual Servers. They must use the Internet IP Address (the IP Address allocated to you by your ISP).
e.g.

http://203.70.212.52
ftp://203.70.212.52

It is more convenient if you are using a Fixed IP Address from your ISP, rather than Dynamic. However, you can use the *Dynamic DNS* feature to allow users to connect to your Virtual Servers using a URL, rather than an IP Address.



Note!

From the Internet, **ALL** Virtual Servers have the IP Address allocated by your ISP

VPN (IPSec)

The VPN (Virtual Private Network) feature in the ADE-4300/ADW-4300 allows you to create a VPN connection between 2 ADE-4300/ADW-4300s, or a remote PC to establish a VPN connection to the ADE-4300/ADW-4300.

To establish a VPN connection from a remote PC to the ADE-4300/ADW-4300, you need suitable (IPSec) VPN client software on your PC.

For more information about VPNs, please refer to **Appendix C - About VPNs**.

VPN Policies

A "VPN Policy" contains all the configuration data for a particular VPN connection. Generally, you will have to create one policy for each site you wish to connect to. The remote VPN Gateway (or client) needs to have matching configuration.

- Traffic covered by an enabled policy will automatically be sent via a VPN tunnel. If the VPN tunnel does not exist, it will be created.
- The VPN tunnel is created according to the parameters in the SA (Security Association).
- The remote VPN Endpoint must have a matching SA, or it will refuse the connection.

There are 2 types of VPN Policies:

- **Manual** - All settings (including the keys) for the VPN tunnel are manually input at each end (both VPN Endpoints).
- **Auto** - Some parameters for the VPN tunnel are generated automatically. This requires using the IKE (Internet Key Exchange) protocol to perform negotiations between the 2 VPN Endpoints.

VPN Policies Screen

This screen is displayed when you select **VPN** on the **Advanced** menu. It allows you to create, modify and manage your VPN Policies.

If you have not created any policies, the Policy Table will be empty.

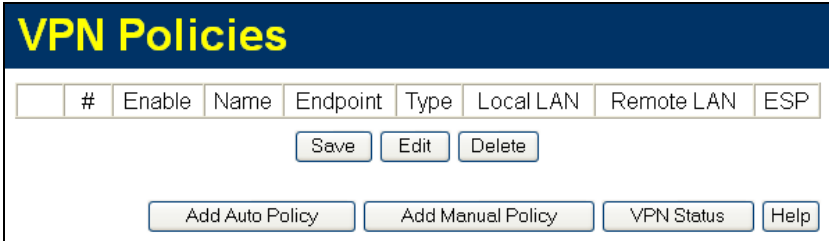


Figure 62: VPN Policies Screen

Data - VPN Policies Screen

Policy Table	<p>The Policy Table contains the following data</p> <ul style="list-style-type: none">• Enable - Use this checkbox to Enable or Disable a Policy as required. Click "Save" after making any changes.• Name - Each policy is given a unique name to identify it. This name is not known to the remote VPN endpoint; it is used only to assist managing your policies.• Endpoint - The address of the remote VPN endpoint.• Type - The Type is "Auto" or "Manual" as explained above.• Local LAN - IP address or subnet on your local LAN. Traffic must be from (or to) these addresses to be covered by this policy.• Remote LAN - IP address or subnet on the remote LAN. Traffic must be to (or from) these addresses to be covered by this policy.• ESP - ESP (Encapsulating Security Payload) encryption protocol used for the VPN data.
Buttons	
Save	Save any changes to the "Enable" setting for each policy.
Edit	Edit (modify) the selected policy. (Select a policy by clicking on the radio button.)
Delete	Delete the selected policy. (Select a policy by clicking on the radio button.)
Add Auto Policy	<p>Change to the input screen for an "Auto" policy. See the following section for details.</p> <p>When the new policy is saved, it will appear in the bottom row of the Policy Table.</p>
Add Manual Policy	<p>Change to the input screen for an "Manual" policy. See the following section for details.</p> <p>When the new policy is saved, it will appear in the bottom row of the Policy Table.</p>

VPN Status	View details of each current VPN Tunnel (connection) in a sub-window. You also have the option of viewing the VPN Log.
-------------------	--

VPN Auto Policy Screen

This screen is displayed when you click the *Add Auto Policy* button on the **VPN Policies** screen, or when you edit an existing Auto Policy. It allows you to define or edit an "Auto" VPN policy.

An "Auto" VPN policy uses the IKE (Internet Key Protocol) to exchange and negotiate parameters for the IPsec SA (Security Association). Because of this negotiation, it is not necessary for all settings on this VPN Gateway to match the settings on the remote VPN endpoint. Where settings must match, this is indicated.

VPN - Auto Policy

General

Policy Name:
Remote VPN Endpoint
Address Type:
Dynamic IP address
Address Data:
n/a
☒ NetBIOS Enable

Local LAN

IP Address
Subnet address
IP address:
192 . 168 . 0 . 1
Subnet Mask:
255 . 255 . 255 . 0

Remote LAN

IP Address
Single PC - no Subnet
IP address:
Subnet Mask:

IKE

Direction
Responder only
Exchange Mode
Main Mode
Diffie-Hellman (DH) Group
Auto
Local Identity Type
WAN IP Address
Data
n/a
Remote Identity Type
IP Address
Data
n/a

SA Parameters

Encryption:
3DES
Authentication:
Auto
Pre-shared Key:
SA Life Time:
28800 (Seconds)
☐ Enable PFS (Perfect Forward Security)

Back
Save
Cancel
Help

Figure 63: VPN-Auto Policy Screen

Data - VPN-Auto Policy Screen

General	
Policy Name	Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.
Remote VPN Endpoint	<p>If the remote endpoint has a dynamic IP address, select "Dynamic IP address". No "Address Data" input is required. Otherwise, select the desired option (IP address or Domain Name) and enter the address of the remote VPN endpoint you wish to connect to.</p> <p>Note: The remote VPN endpoint must have this VPN Gateway's address entered as its "Remote VPN Endpoint".</p>
NetBIOS Enable	Check this if you wish NETBIOS traffic to be forwarded over the VPN tunnel. The NETBIOS protocol is used by Microsoft Networking.
Local LAN	
Local LAN	<p>This identifies which PCs on your LAN are covered by this policy. For each selection, data must be provided as follows:</p> <ul style="list-style-type: none"> • Single address Enter an IP address in the "IP address" field. Typically, this setting is used when you wish to make a single Server on your LAN available to remote users. • Subnet address Enter an IP address in the "IP address" field, and the desired network mask in the "Subnet Mask" field. <p>The remote VPN endpoint must have these IP addresses entered as its "Remote" addresses.</p>
Remote LAN	
Remote LAN	<p>This identifies which PCs on the remote LAN are covered by this policy. For each selection, data must be provided as follows:</p> <ul style="list-style-type: none"> • Single PC - no subnet Select this option if there is no LAN (only a single PC) at the remote endpoint. If this option is selected, no additional data is required. • Single address Enter an IP address in the "IP address" field. This must be an address on the remote LAN. Typically, this setting is used when you wish to access a server on the remote LAN. • Subnet address Enter an IP address in the "IP address" field, and the desired network mask in the "Subnet Mask" field. <p>The remote VPN endpoint must have these IP addresses entered as its "Local" addresses.</p>

IKE	
Direction	<p>This setting is used when determining if the IKE policy matches the current traffic. Select the desired option.</p> <ul style="list-style-type: none"> • Responder only - Incoming connections are allowed, but outgoing connections will be blocked. • Initiator and Responder - Both incoming and outgoing connections are allowed.
Exchange Mode	<p>IPSec has 2 possibilities - "Main Mode" and "Aggressive Mode".</p> <p>Currently, only "Main Mode" is supported. Ensure the remote VPN endpoint is set to use "Main Mode".</p>
Diffie-Hellman (DH) Group	<p>The Diffie-Hellman algorithm is used when exchanging keys. The DH Group setting determines the number of bit size used in the exchange. This value must match the value used on the remote VPN Gateway.</p>
Local Identity Type	<p>Select the desired option to match the "Remote Identity Type" setting on the remote VPN endpoint.</p> <ul style="list-style-type: none"> • WAN IP Address - your Internet IP address. • Fully Qualified Domain Name - your domain name. • Fully Qualified User Name - your name, E-mail address, or other ID.
Remote Identity Type	<p>Select the desired option to match the "Local Identity Type" setting on the remote VPN endpoint.</p> <ul style="list-style-type: none"> • IP Address - The Internet IP address of the remote VPN endpoint. • Fully Qualified Domain Name - the Domain name of the remote VPN endpoint. • Fully Qualified User Name - the name, E-mail address, or other ID of the remote VPN endpoint.
Remote Identity Data	<p>Enter the data for the selection above. (If "IP Address" is selected, no input is required.)</p>
SA Parameters	
Encryption	<p>Encryption Algorithm used for both IKE and IPSec. This setting must match the setting used on the remote VPN Gateway.</p>
Authentication	<p>Authentication Algorithm used for both IKE and IPSec. This setting must match the setting used on the remote VPN Gateway.</p>
Pre-shared Key	<p>The key must be entered both here and on the remote VPN Gateway. This method does not require using a CA (Certificate Authority).</p>
SA Life Time	<p>This determines the time interval before the SA (Security Association) expires. (It will automatically be re-established if necessary.) While using a short time period (or data amount) increases security, it also degrades performance. It is common to use periods over an hour (3600 seconds) for the SA Life Time. This setting applies to both IKE and IPSec SAs.</p>

IPSec PFS (Perfect Forward Secrecy)	<p>If enabled, security is enhanced by ensuring that the key is changed at regular intervals. Also, even if one key is broken, subsequent keys are no easier to break. (Each key has no relationship to the previous key.)</p> <p>This setting applies to both IKE and IPSec SAs. When configuring the remote endpoint to match this setting, you may have to specify the "Key Group" used. For this device, the "Key Group" is the same as the "DH Group" setting in the IKE section.</p>
--	--

VPN- Manual Policy Screen

This screen is displayed when you click the *Add Manual Policy* button on the **VPN Policies** screen, or when you edit an existing Manual Policy. It allows you to define or edit a "Manual" VPN policy.

An "Manual" VPN policy requires that you enter all data on both VPN endpoints. There is no negotiation between the 2 VPN endpoints.

VPN - Manual Policy

General

Policy Name:

Remote VPN Endpoint

Address Type: Fixed IP Address

Address Data:

☒ NETBIOS Enable

Local LAN

IP Address Subnet address

IP address: . . .

Subnet Mask: . . .

Remote LAN

IP Address Single PC - no subnet

IP address: . . .

Subnet Mask: . . .

ESP Configuration

SPI - Incoming (Hex, 3 Characters)

SPI - Outgoing (Hex, 3 Characters)

Encryption 3DES

Key:

(DES: 8 chars; 3DES: 24 chars)

Authentication SHA-1

Key:

(MD5: 16 chars; SHA-1: 20 chars)

Figure 64: VPN-Manual Policy Screen

Data - VPN-Manual Policy Screen

General	
Policy Name	Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.
Remote VPN Endpoint	Select the desired option (IP address or Domain Name) and enter the address of the remote VPN endpoint you wish to connect to. Note: The remote VPN endpoint must have this VPN Gateway's address entered as its "Remote VPN Endpoint".

NETBIOS Enable	Check this if you wish NETBIOS traffic to be forwarded over the VPN tunnel. The NETBIOS protocol is used by Microsoft Networking.
Local LAN	
Local LAN	<p>This identifies which PCs on your LAN are covered by this policy. For each selection, data must be provided as follows:</p> <ul style="list-style-type: none"> • Single address Enter an IP address in the "IP address" field. Typically, this setting is used when you wish to make a single Server on your LAN available to remote users. • Subnet address Enter an IP address in the "IP address" field, and the desired network mask in the "Subnet Mask" field. <p>The remote VPN endpoint must have these IP addresses entered as its "Remote" addresses.</p>
Remote LAN	
Remote LAN	<p>This identifies which PCs on the remote LAN are covered by this policy. For each selection, data must be provided as follows:</p> <ul style="list-style-type: none"> • Single PC - no subnet Select this option if there is no LAN (only a single PC) at the remote endpoint. If this option is selected, no additional data is required. • Single address Enter an IP address in the "IP address" field. This must be an address on the remote LAN. Typically, this setting is used when you wish to access a server on the remote LAN. • Subnet address Enter an IP address in the "IP address" field, and the desired network mask in the "Subnet Mask" field. <p>The remote VPN endpoint must have these IP addresses entered as its "Local" addresses.</p>
ESP Configuration	
SPI	Enter the required SPIs. Each policy must have unique SPIs. These settings must match the remote VPN endpoint. Note that the "in" setting here must match the "out" setting on the remote VPN endpoint, and the "out" setting here must match the "in" setting on the remote VPN endpoint.
Encryption	<p>Select the desired Encryption Algorithm, and enter the key in the field provided.</p> <ul style="list-style-type: none"> • For DES, the key should be 8 ASCII characters (16 Hex characters). • For 3DES, the key should be 24 ASCII characters (48 Hex characters).

Authentication	<p>Select the desired Authentication Algorithm, and enter the key in the field provided.</p> <ul style="list-style-type: none">• For MD5, the key should be 16 ASCII characters (32 Hex characters).• For SHA-1, the key should be 20 ASCII (40 Hex characters).
-----------------------	---

VPN Status Screen

This screen is displayed when you click the VPN Log button on the VPN Policies screen, or on the Status screen.

This screen allows you to view details of each current VPN Tunnel (connection). If there are no current connections, the status table will be empty.

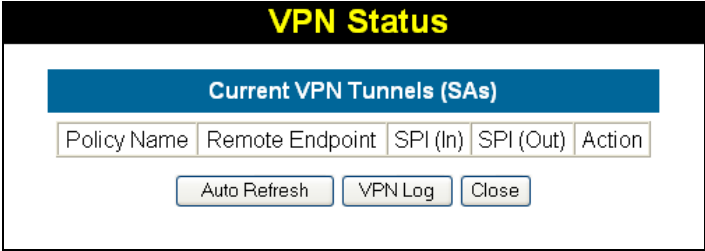


Figure 65: VPN-Status Screen

Data - VPN Status Screen

Tunnel Table	<p>This table contains the following data about each current connection.</p> <ul style="list-style-type: none">• Policy Name - The name of the policy. When a policy is created, it must be given a unique name to identify it.• Remote Endpoint - The address of the remote VPN endpoint.• SPI (In) - This is a unique index number to identify the incoming connection. For "Auto" policies, the SPI is automatically generated. For "Manual" policies, the SPI must be entered when the policy is configured.• SPI (Out) - This is a unique index number to identify the outgoing connection. For "Auto" policies, the SPI is automatically generated. For "Manual" policies, the SPI must be entered when the policy is configured.• Action - This column will contain a button which allows you to break (terminate) the current the VPN connection.
Buttons	
Auto Refresh	<p>Use this to Enable or Disable auto-refresh for this screen. If enabled, the screen will be updated every few seconds.</p> <p>The status bar on the bottom on the screen will indicate if auto-refresh is enabled or disabled.</p>
VPN Log	<p>Click this button to switch to the VPN log screen.</p> <p>The VPN log shows details of each connection as it is created.</p>

Microsoft VPN

Microsoft VPN uses the Microsoft VPN Adapter which is provided in recent versions of Windows. This feature can be used to provide remote access to your LAN by individual PCs. This method provides an alternative to using IPsec VPN, which is described in the previous chapter. Using Microsoft VPN provides easier setup than using IPsec VPN.

Microsoft VPN Screen

ADE-4300 / ADW-4300 incorporates a PPTP (Peer-to-Peer Tunneling Protocol) server which is compatible with the "VPN Adapter" provided with recent versions of Microsoft Windows. Remote Windows clients are able to connect to this Server. Once connected, they can access the LAN as if they connected locally.

This screen is displayed when you select Microsoft VPN on the Advanced menu.

Microsoft VPN

PPTP Server

This Server is compatible with the "VPN Adapter" provided with recent versions of Microsoft Windows.

☐ Enable PPTP (VPN) Server

☐ Auto-disconnect Idle Time-Out: 30 min

VPN Server Status

Remote Users

Existing Users

Delete Delete All

Add New User

Login Name:

Login Password:

Verify Password:

Add User Clear Form

Save Cancel Help

Figure 66: Microsoft VPN Screen

Data – Microsoft VPN Screen

PPTP Server	
Enable	Use this checkbox to enable or disable this feature as required. To allow connection by remote Windows clients, you must enable this feature, and enter the client details (on the Clients screen) to allow them to login to this Server.
Auto-disconnect Idle Time-out	Use this checkbox to enable or disable this feature as required. To disconnect PPTP connection automatically when the login time reach the idle time.
Remote Users	
Login Name	Enter the login name. The remote user must provide this name when they connect. The name must not contain spaces, punctuation, or special characters.
Login Password	Enter the login password. The remote user must provide this password when they connect.
Verify Password	Re-enter the password above.
Buttons	
VPN Server Status	Click this button to open a sub-window and view the details of each current PPTP connection.
Delete	Use this to delete the selected user if required.
Delete All	Use this to delete whole users.
Add User	Use this to save the data in the "Properties" area as a new entry. (If a user is selected in the "Existing User" list, the selection is ignored.)
Clear Form	Use this to prepare the form for a new entry. Any existing data will be cleared.

VPN Server Status Screen

This screen is displayed when you click the VPN Server Status button on the Micro-soft VPN screen.



Figure 67: Microsoft VPN Status Screen

Data - Microsoft VPN Status Screen

Connection Table	<p>This table contains the following data about each current connection.</p> <ul style="list-style-type: none"> • User Name – The login name. • Remote IP - The IP address of the remote client. • Local IP – ADE-4300/ADW-4300 will allocate a local IP address to remote client when user login. • Start Time – This displays the start time when remote client login to the ADE-4300/ADW-4300.. • Action - This column will contain a button which allows you to break (terminate) the PPTP connection.
Server Log	
Auto Refresh	<p>Use this to Enable or Disable auto-refresh for this screen. If enabled, the screen will be updated every few seconds.</p> <p>The status bar on the bottom on the screen will indicate if auto-refresh is enabled or disabled.</p>
View Log	<p>This displays details of each connection or connection attempt.</p> <p>You can use the Clear Log button to re-start the log, making new messages easier to read.</p>

Windows Client Setup

To connect to the PPTP (VPN) Server in the VPN Broadband Gateway:

- The Microsoft VPN feature in the VPN Broadband Gateway must be enabled and configured, as described in the previous section.
- Each user must have a login (username and password) on the VPN client database on the VPN Broadband Gateway.
- The remote client PC must be configured as described in the following sections.
- It is assumed that remote users have a Broadband (not dial-up) connection to the Internet.

Windows 98/ME

1. Click Start - Settings - Dial-up Networking
2. Select Make New Connection
3. Type a name for this connection, and ensure that "Microsoft VPN Adapter" is selected. Click "Next" to continue.



Figure 68: Windows ME VPN Adapter

4. Enter the Internet IP address or domain name of this device. (If you don't have a fixed IP address, you can use a Dynamic DNS service to obtain a domain name.) Click "Next" to continue.

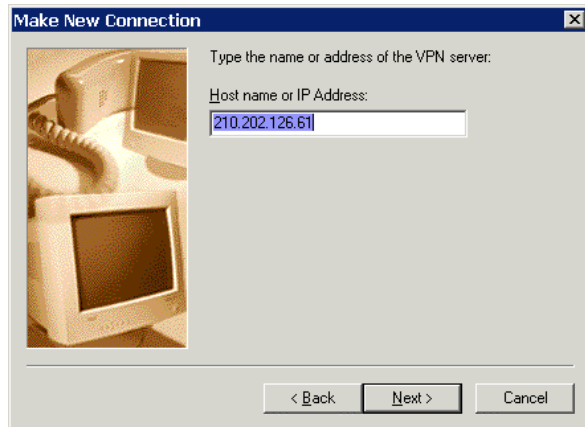


Figure 69: Windows ME VPN Remote Host

5. Click "Finish" to exit the Wizard.
The new entry will now be listed in "Dial-up Networking".

If necessary, you can change the settings for this connection by right-clicking on it, and selecting Properties.

To force all outgoing traffic to be sent via VPN, enable the setting This is the default Internet connection on the Dialing tab. (Do NOT enable this setting if using Dial-up or PPPoE client software.)

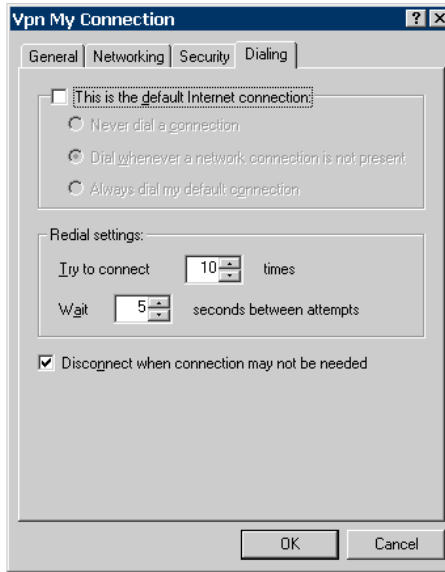


Figure 70: Windows ME VPN Dialing Properties

To establish a connection:

1. Ensure you are connected to the Internet.
2. Select Start - Settings - Dial-up Networking
3. Double-click the new VPN entry in Dial-up Networking.
4. Enter your User name and Password, as recorded in the Client database on ADE-4300 / ADW-4300.
5. Click the "Connect" button.

Windows 2000

Ensure you have logged on with Administrator rights before attempting this procedure.

1. Open "Network Connections", and start the "New Connection" Wizard.
2. Select the VPN option ("Connect to a private network through the Internet"), as shown below, and click Next.

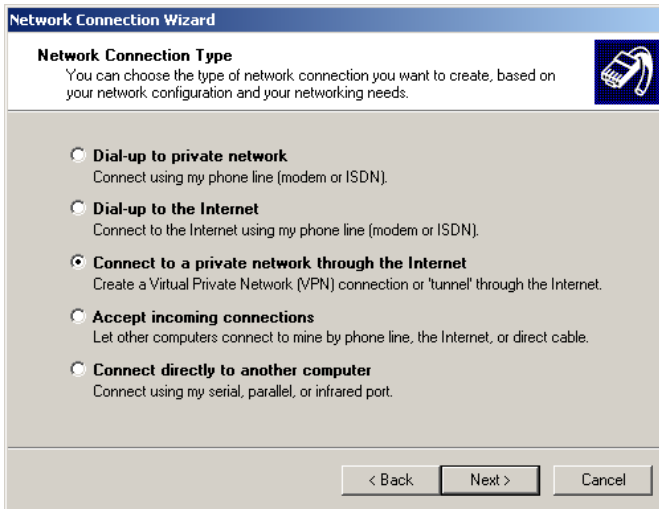


Figure 71: Windows 2000 Network Connection

3. On the screen below:

- Select "Do not dial the initial connection" if Internet access is via the LAN.
- If using a PPPoE software client, select "Automatically dial this initial connection" and select the PPPoE connection.
- Click Next to continue.

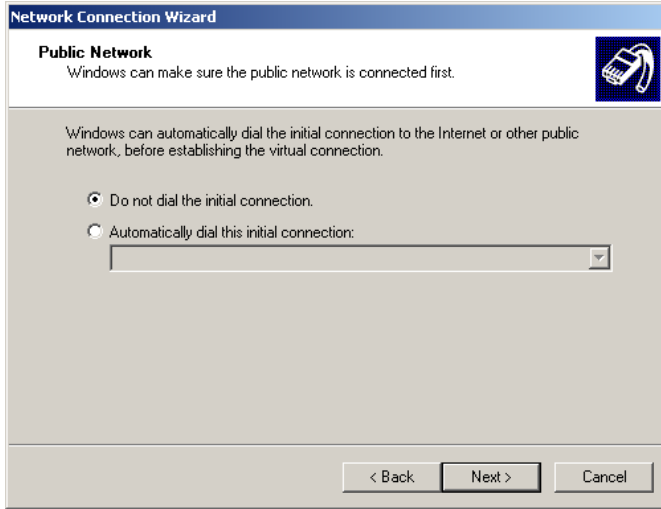


Figure 72: Windows 2000 Public Network

4. On the screen below, enter the Domain Name or Internet IP address of ADE-4300 / ADW-4300 you wish to connect to. Click Next to continue.

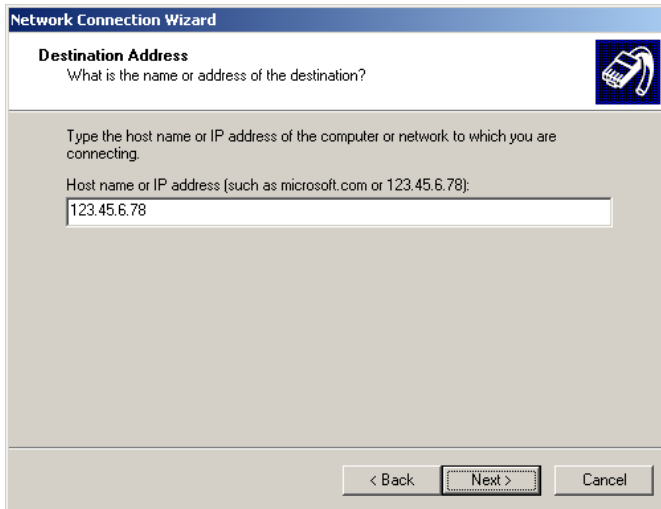


Figure 73: Windows 2000 VPN Host

5. Choose whether to allow this connection for everyone, or only for yourself, as required. Click Next to continue.

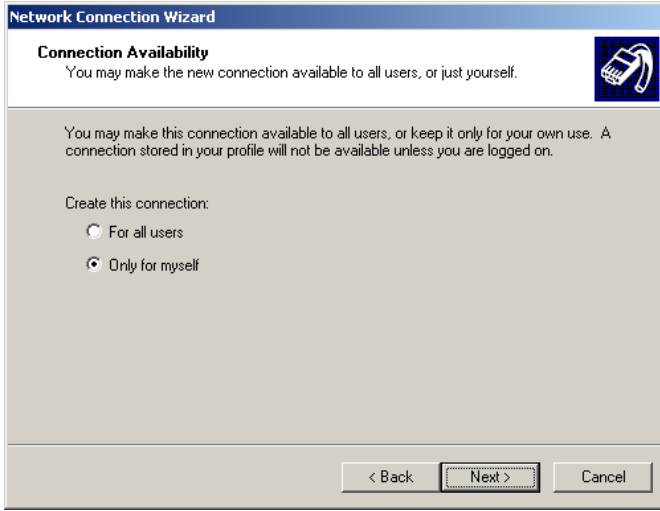


Figure 74: Windows 2000 Connection Availability

6. Enter a suitable name, and click "Finish" to save and exit.

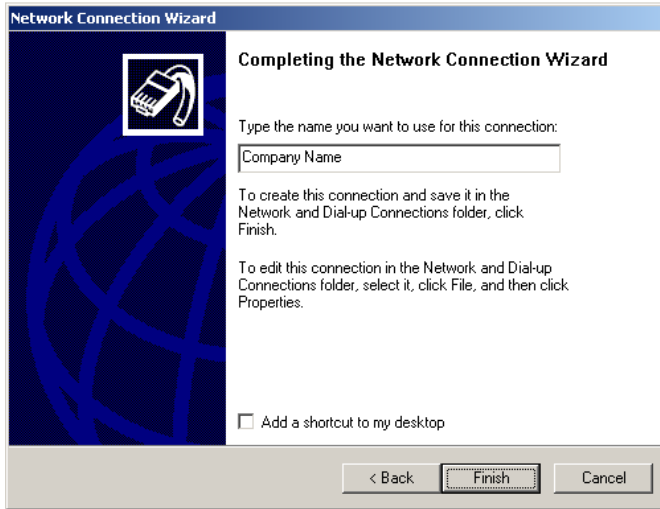


Figure 75: Windows 2000 Finish Wizard

Setup is now complete.

To establish a connection:

- 1 Right-click the connection in "Network Connections", and select "Connect".
- 2 You will then be prompted for the username and password. Enter the username and password assigned to you, as recorded in the VPN client database on ADE-4300 / ADW-4300.
- 3 You can choose to have Windows remember the password if desired, so you do not have to enter it again.

Changing the connection settings

The PPTP (VPN) Server in ADE-4300 / ADW-4300 is designed to work with the default Windows settings.

- If necessary, you can change the Windows settings by right-clicking the VPN connection in Network Connections, and selecting Properties.

- The Properties dialog has a Networking tab with a "Type of VPN" setting. If you have trouble connecting, you can change this setting from "Automatic" to "PPTP VPN".

Windows XP

Ensure you have logged on with Administrator rights before attempting this procedure.

1. Open Network Connections (Start-Settings-Network Connections), and start the New Connection Wizard.
2. Select the option "Connect to the network at my workplace", as shown below, and click Next.

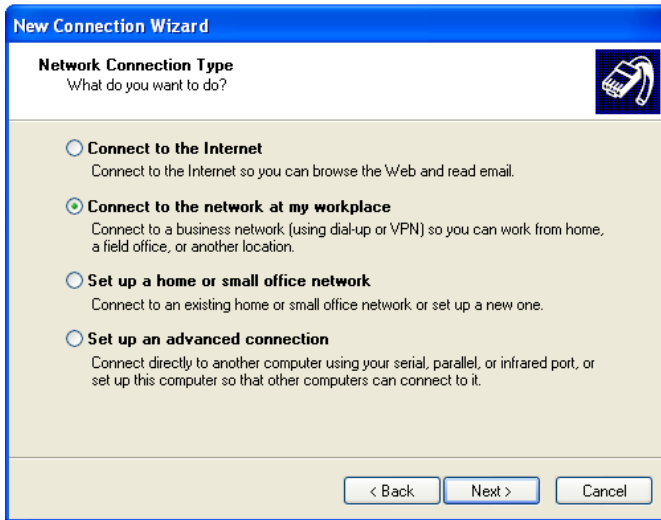


Figure 76: Windows XP Network Connection Type

3. On the next screen, shown below, select the "Virtual Private Network connection" option. Click Next to continue.

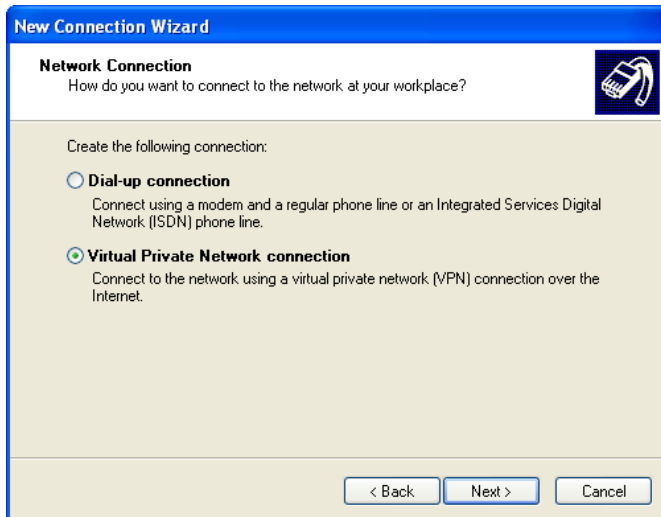


Figure 77: Windows XP Network Connection

4. Enter a suitable name for this connection. Click Next to continue.

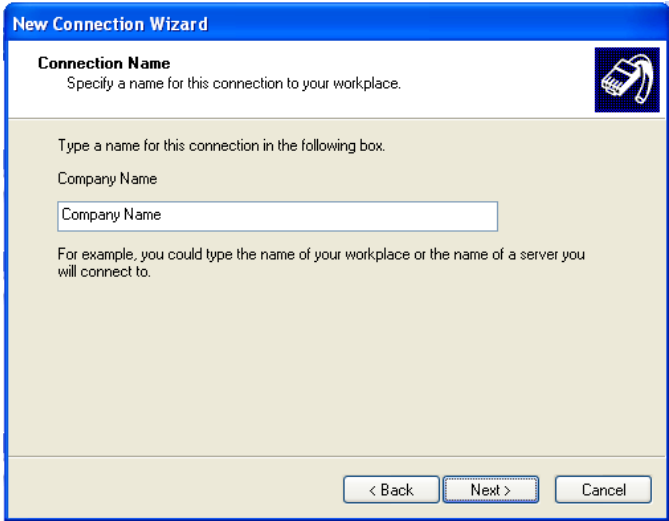


Figure 78: Windows XP Connection Name

5. On the screen below, select "Do not dial the initial connection". Click Next to continue.

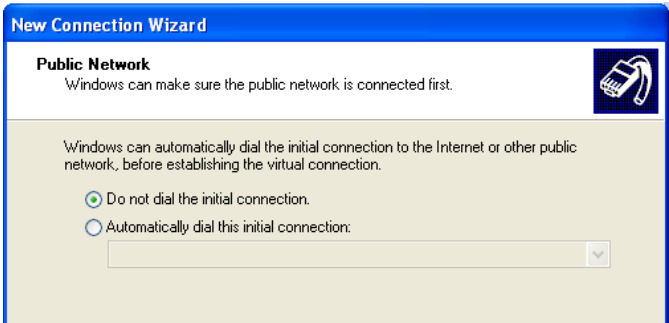


Figure 79: Windows XP Public Network

6. On the screen below, enter the Domain Name or Internet IP address of ADE-4300 / ADW-4300 you wish to connect to. Click Next to continue.

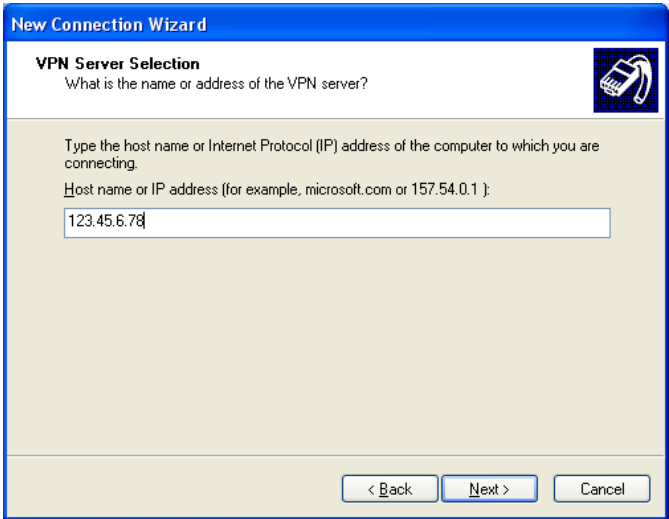


Figure 80: Windows XP VPN Server

7. Choose whether to allow this connection for everyone, or only for yourself, as required. Click Next to continue.

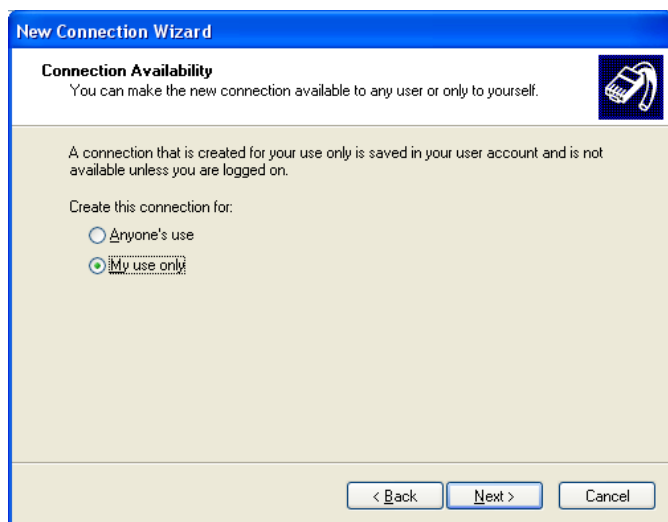


Figure 81: Windows XP Connection Availability

8. On the final screen, click Finish to save and exit.

Setup is now complete.

To establish a connection:

- 1 Right-click the connection in "Network Connections", and select "Connect".
- 2 You will then be prompted for the username and password. Enter the username and password assigned to you, as recorded in the VPN client database on ADE-4300 / ADW-4300.
- 3 You can choose to have Windows remember the password if desired, so you do not have to enter it again.

Changing the connection settings

The PPTP (VPN) Server in ADE-4300 / ADW-4300 is designed to work with the default Windows settings.

- If necessary, you can change the Windows settings by right-clicking the VPN connection in Network Connections, and selecting Properties.
- The Properties dialog has a Networking tab with a "Type of VPN" setting. If you have trouble connecting, you can change this setting from "Automatic" to "PPTP VPN".

SNMP

Simple Network Management Protocol (SNMP) is the protocol which enable administrator to monitor network and bandwidth usage as well as various other network parameters like system information and port usages, providing system administrators with live readings and periodical usage trends to optimize the network efficiency.

SNMP Screen

Select *Advanced* on the main menu, then *SNMP*, to see a screen like the following:

SNMP

SNMP Service

☐ Enable SNMP support

SNMP (Simple Network Management Protocol) software must be installed on your PC.

SNMP Data

Community Name

SysContact

SysName

SysLocation

Save Cancel Help

Figure 82: SNMP Screen

Data - SNMP Screen

SNMP Service	
Enable SNMP support	Enable or disable the SNMP feature as required.
SNMP Data	
Community Name	Enter the Community Name as the Read Community which SNMP Software will use it to access ADE-4300/ADW-4300. Once the string name is matched, user will be able to view the SNMP data.
SysContact	Specify a name in any string to be the System Contact.
SysName	Specify a name in any string to be the System Name.
SysLocation	Specify a name in any string to be the System Location.

Chapter 7



Advanced Administration

This Chapter explains the settings available via the "Administration" section of the menu.

Overview

Normally, it is not necessary to use these screens, or change any settings. These screens and settings are provided to deal with non-standard situations, or to provide additional options for advanced users.

The available settings and features are:

PC Database	This is the list of PCs shown when you select the "DMZ PC" or a "Virtual Server". This database is maintained automatically, but you can add and delete entries for PCs which use a Fixed (Static) IP Address.
Config File	Backup or restore the configuration file for the ADE-4300/ADW-4300. This file contains all the configuration data.
Logging & Email	View or clear all logs, set E-Mailing of log files and alerts.
Diagnostics	Perform a Ping or DNS Lookup.
Remote Admin	Allow settings to be changed from the Internet..
Routing	Only required if your LAN has other Routers or Gateways.
Upgrade Firmware	Upgrade the Firmware (software) installed in your ADE-4300/ADW-4300.

PC Database

The PC Database is used whenever you need to select a PC (e.g. for the "DMZ" PC).

- It eliminates the need to enter IP addresses.
- Also, you do not need to use fixed IP addresses on your LAN.

However, if you do use a fixed IP address on some devices on your LAN, you should enter details of each such device into the PC database, using the PC Database screen.

PC Database Screen

An example **PC Database** screen is shown below.

PC Database

DHCP Clients are automatically added and updated.
If not listed, try restarting the PC.

PCs using a Fixed IP address can be added and deleted below.

Known PCs
Secada 192.168.0.3 (LAN) 00:30:4F:30:D2:B7 (DHCP)

< Add

Delete

Name:
IP Address:

Refresh Generate Report

Advanced Administration Help

Figure 83: PC Database

- PCs which are "DHCP Clients" are automatically added to the database, and updated as required.
- By default, non-Server versions of Windows act as "DHCP Clients"; this setting is called "Obtain an IP Address automatically".
- The ADE-4300/ADW-4300 uses the "Hardware Address" to identify each PC, not the name or IP address. The "Hardware Address" can only change if you change the PC's network card or adapter.
- This system means you do NOT need to use Fixed (static) IP addresses on your LAN. However, you can add PCs using Fixed (static) IP Addresses to the PC database if required.

Data - PC Database Screen

Known PCs	This lists all current entries. Data displayed is <i>name (IP Address) type</i> . The "type" indicates whether the PC is connected to the LAN.
Name	If adding a new PC to the list, enter its name here. It is best if this matches the PC's "hostname".
IP Address	Enter the IP Address of the PC. The PC will be sent a "ping" to determine its hardware address. If the PC is not available (not connected, or not powered On) you will not be able to add it.
Buttons	
Add	This will add the new PC to the list. The PC will be sent a "ping" to determine its hardware address. If the PC is not available (not connected, or not powered On) you will not be able to add it.
Delete	Delete the selected PC from the list. This should be done in 2 situations: <ul style="list-style-type: none">• The PC has been removed from your LAN.• The entry is incorrect.
Refresh	Update the data on screen.
Generate Report	Display a read-only list showing full details of all entries in the PC database.
Advanced Administration	View the Advanced version of the PC database screen - PC Database (Admin) . See below for details.

PC Database - Advanced

This screen is displayed if the "Advanced Administration" button on the *PC Database* is clicked. It provides more control than the standard *PC Database* screen.

PC Database - Advanced

Any PC may be added, edited or deleted. If adding a PC which is not connected and On, you must provide the MAC (hardware) address

Known PCs

kang-chang 192.168.0.2 (LAN) 00:01:29:F1:18:A6 (DHCP)

Edit

Delete

PC Properties

Name:

IP Address:

☐ Automatic (DHCP Client)

☒ DHCP Client - reserved IP address:

192

168

0

☒ Fixed IP address (set on PC):

MAC Address:

☐ Automatic discovery (PC must be available on LAN)

☒ MAC address is

Clear Form

Add as New Entry

Update Selected PC

Refresh

Generate Report

Standard Screen

Help

Figure 84: PC Database (Admin)

Data - Advanced PC Database

Known PCs	This lists all current entries. Data displayed is <i>name (IP Address) type</i> . The "type" indicates whether the PC is connected to the LAN.
PC Properties	
Name	If adding a new PC to the list, enter its name here. It is best if this matches the PC's "hostname".

102

IP Address	<p>Select the appropriate option:</p> <ul style="list-style-type: none"> • Automatic - The PC is set to be a DHCP client (Windows: "Obtain an IP address automatically"). The ADE-4300/ADW-4300 will allocate an IP address to this PC when requested to do so. The IP address could change, but normally won't. • DCHP Client - Reserved IP Address - Select this if the PC is set to be a DCHP client, and you wish to guarantee that the ADE-4300/ADW-4300 will always allocate the same IP Address to this PC. Enter the required IP address. • Fixed IP Address - Select this if the PC is using a Fixed (Static) IP address. Enter the IP address allocated to the PC. (The PC itself must be configured to use this IP address.)
MAC Address	<p>Select the appropriate option</p> <ul style="list-style-type: none"> • Automatic discovery - Select this to have the ADE-4300/ADW-4300 contact the PC and find its MAC address. This is only possible if the PC is connected to the LAN and powered On. • MAC address is - Enter the MAC address on the PC. The MAC address is also called the "Hardware Address", "Physical Address", or "Network Adapter Address". The ADE-4300/ADW-4300 uses this to provide a unique identifier for each PC. Because of this, the MAC address can NOT be left blank.
Buttons	
Add as New Entry	Add a new PC to the list, using the data in the "Properties" box. If "Automatic discovery" (for MAC address) is selected, the PC will be sent a "ping" to determine its hardware address. This will fail unless the PC is connected to the LAN, and powered on.
Update Selected PC	Update (modify) the selected PC, using the data in the "Properties" box.
Clear Form	Clear the "Properties" box, ready for entering data for a new PC.
Refresh	Update the data on screen.
Generate Report	Display a read-only list showing full details of all entries in the PC database.
Standard Screen	Click this to view the standard PC Database screen.

Config File

This feature allows you to download the current settings from the ADE-4300/ADW-4300, and save them to a file on your PC.

You can restore a previously-downloaded configuration file to the ADE-4300/ADW-4300, by uploading it to the ADE-4300/ADW-4300.

This screen also allows you to set the ADE-4300/ADW-4300 back to its factory default configuration. Any existing settings will be deleted.

An example **Config File** screen is shown below.

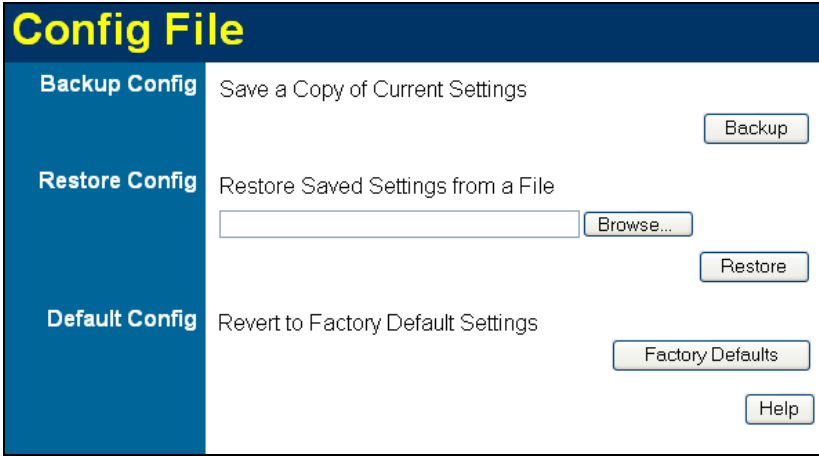


Figure 85: Config File Screen

Data - Config File Screen

Backup Config	Use this to download a copy of the current configuration, and store the file on your PC. Click <i>Download</i> to start the download.
Restore Config	<p>This allows you to restore a previously-saved configuration file back to the ADE-4300/ADW-4300.</p> <p>Click <i>Browse</i> to select the configuration file, then click <i>Restore</i> to upload the configuration file.</p> <p>WARNING !</p> <p>Uploading a configuration file will destroy (overwrite) ALL of the existing settings.</p>
Default Config	<p>Clicking the <i>Factory Defaults</i> button will reset the ADE-4300/ADW-4300 to its factory default settings.</p> <p>WARNING !</p> <p>This will delete ALL of the existing settings.</p>

Logging

The Logs record various types of activity on the ADE-4300/ADW-4300. This data is useful for troubleshooting, but enabling all logs will generate a large amount of data and adversely affect performance.

Since only a limited amount of log data can be stored in the ADE-4300/ADW-4300, log data can also be E-mailed to your PC. Use the **E-mail** screen to configure this feature.

Logs

Logs

Current time: 2002-09-08 12:55:19

Sun, 2002-09-08 12:08:31 - Administrator login

Sun, 2002-09-08 12:00:00 - Router start up

Refresh

Clear Log

Send Log

Include in Log

☒ Attempted access to blocked sites

☒ Connections to the Web-based interface of this Router

☒ Router operation (start up, get time etc)

☒ Known DoS attacks and Port Scans

Syslog

☒ Disable

☐ Broadcast on LAN

☐ Send to this Syslog Server:

Save

Cancel

Help

Figure 86: Logging Screen

Data - Logging Screen

Logs	
Current Time	The current time on the ADE-4300/ADW-4300 is displayed.
Log Data	Current log data is displayed in this panel.
Buttons	<div>There are three (3) buttons</div> <ul style="list-style-type: none">Refresh - Update the log data.Clear Log - Clear the log, and restart it. This makes new messages easier to read.Send Log - E-mail the log immediately. This is only functional if the E-mail screen has been configured.

Logs	
Include (Check-boxes)	<p>Use these checkboxes to determine which events are included in the log. Checking all options will increase the size of the log, so it is good practice to disable any events which are not really required.</p> <ul style="list-style-type: none"> • Attempted access to blocked sites - If checked, attempted Internet accesses which were blocked are logged. • Connections to the Web-based interface of this Router - If checked, this will log connections TO this Router, rather than through this Router to the Internet. • Router operation - If checked, other Router operations (not covered by the selections above) will be logged. • Known DoS attacks and Port Scans - If checked, Denial of Service attacks, as well as port scans, will be logged.
Syslog	
Disable	Data is not sent to a Syslog Server.
Broadcast on LAN	The Syslog data is broadcast, rather than sent to a specific Syslog server. Use this if your Syslog Server does not have a fixed IP address.
Syslog	If your Syslog server has a fixed IP address, select this option, and enter the IP address of your Syslog server.

E-mail

This screen allows you to E-mail Logs and Alerts. A sample screen is shown below.

E-Mail

E-mail Notification

☐ Turn E-mail Notification On

Send to this E-mail Address:

Outgoing (SMTP) Mail Server:

☐ My SMTP Mail Server requires authentication

User Name:

Password:

E-mail Alerts

Send E-Mail alerts immediately

☒ If a DoS attack is detected.

☒ If a Port Scan is detected.

☒ If someone attempts to access a blocked site.

E-mail Logs

Send Logs According to this Schedule

Hourly

Day

Time ☒ a.m. ☐ p.m.

Figure 87: E-mail Screen

Data - E-mail Screen

E-Mail Notification	
Turn E-mail Notification on	Check this box to enable this feature. If enabled, the E-mail address information (below) must be provided.
Send to this E-mail address	Enter the E-mail address the Log is to be sent to. The E-mail will also show this address as the Sender's address.
Outgoing (SMTP) Mail Server	Enter the address or IP address of the SMTP (Simple Mail Transport Protocol) Server you use for outgoing E-mail.
My SMTP Mail Server requires authentication	To stop spammers, many SMTP mail servers require you to log in to send mail. In this case, enable this checkbox, and enter the login information (User name and Password) in the fields below.
User Name	If you have enabled "My SMTP Mail Server requires authentication" above, enter the User Name required to login to your SMTP Server.
Password	If you have enabled "My SMTP Mail Server requires authentication" above, enter the password required to login to your SMTP Server.

E-mail Alerts	
Send E-mail alerts immediately	<p>You can choose to have alerts E-mailed to you, by checking the desired checkboxes. The ADE-4300/ADW-4300 can send an immediate alert when it detects a significant security incident such as</p> <ul style="list-style-type: none"> • A known hacker attack is directed at your IP address • A computer on the Internet scans your IP address for open ports • Someone on your LAN (Local Area Network) tries to visit a blocked site.
E-mail Logs	
Send Logs	<p>Select the desired option for sending the log by E-mail.</p> <ul style="list-style-type: none"> • Never (default) - This feature is disabled; Logs are not sent. • When log is full - The time is not fixed. The log will be sent when the log is full, which will depend on the volume of traffic. • Hourly, Daily, Weekly... - The log is sent on the interval specified. • If Daily is selected, the log is sent at the time specified. Select the time of day you wish the E-mail to be sent. • If Weekly is selected, the log is sent once per week, on the specified day, at the specified time. Select the day and the time of day you wish the E-mail to be sent. <p>Note:</p> <p>If the log is full before the time specified to send it, it will be sent regardless of the day and time specified.</p>

Diagnostics

This screen allows you to perform a "Ping" or a "DNS lookup". These activities can be useful in solving network problems.

An example **Network Diagnostics** screen is shown below.

Ping

DNS Lookup

Routing

IP Address:

Internet Name:

IP address:

DNS Server:

Display the Routing Table

Ping

Lookup

Display

Help

Figure 88: Network Diagnostics Screen

Data - Network Diagnostics Screen

Ping	
Ping this IP Address	Enter the IP address you wish to ping. The IP address can be on your LAN, or on the Internet. Note that if the address is on the Internet, and no connection currently exists, you could get a "Timeout" error. In that case, wait a few seconds and try again.
Ping Button	After entering the IP address, click this button to start the "Ping" procedure. The results will be displayed in the <i>Ping Results</i> pane.
DNS Lookup	
Internet name	Enter the Domain name or URL for which you want a DNS (Domain Name Server) lookup. Note that if the address is on the Internet, and no connection currently exists, you could get a "Timeout" error. In that case, wait a few seconds and try again.
Lookup Button	After entering the Domain name/URL, click this button to start the "DNS Lookup" procedure.
Routing	
Display	Click this button to display the internal routing table. This information can be used by Technical Support and other staff who understand Routing Tables.

Remote Administration

If enabled, this feature allows you to manage the ADE-4300/ADW-4300 via the Internet.

Remote Administration

Access Permission

☐ Enable Remote Management

Current IP Address:

Port Number:

Allow Remote Access By:

☒ Everyone

☐ Only This Computer: . . .

☐ IP Address Range : From . . . To . . .

Figure 89: Remote Administration Screen

Data - Remote Administration Screen

Remote Administration	
Enable Remote Management	<p>Check to allow administration/management via the Internet. (To connect, see below).</p> <p>If Disabled, this device will ignore Administration connection attempts from the Internet.</p>
Current IP Address	<p>This is the current address you will use when accessing this device from the Internet. To connect, see details and an example below.</p>
Port Number	<p>Enter a port number between 1 and 65535. The default for HTTP (Web) connections is port 80, but using port 80 will prevent the use of a Web "Virtual Server" on your LAN. So using a different port number is recommended. The default value is 8080.</p> <p>The port number must be specified in your Browser when you connect. See the following section for details.</p>
Access Permission	
Allow Remote Access	<p>Select the desired option.</p> <ul style="list-style-type: none">Everyone - allow access by everyone on the Internet.Only This Computer - allow access by only one IP address. Enter the desired IP address.IP Address Range - allow access from a range of IP addresses on the Internet. Enter a beginning and ending IP address to define the allowed range. <p>For security, you should restrict access to as few external IP addresses as practical.</p>

To connect from a remote PC via the Internet

1. Ensure your Internet connection is established, and start your Web Browser.
2. In the "Address" bar, enter "HTTP://" followed by the Internet IP Address of the ADE-4300/ADW-4300. If the port number is not 80, the port number is also required. (After the IP Address, enter ":" followed by the port number.)

e.g.

`HTTP://123.123.123.123:8080`

This example assumes the WAN IP Address is 123.123.123.123, and the port number is 8080.

3. You will then be prompted for the login name and password for this device.

Routing

Overview

- If you don't have other Routers or Gateways on your LAN, you can ignore the "Routing" page completely.
- If the ADE-4300/ADW-4300 is only acting as a Gateway for the local LAN segment, ignore the "Routing" page even if your LAN has other Routers.
- If your LAN has a standard Router (e.g. Cisco) on your LAN, and the ADE-4300/ADW-4300 is to act as a Gateway for all LAN segments, enable RIP (Routing Information Protocol) and ignore the Static Routing table.
- If your LAN has other Gateways and Routers, and you wish to control which LAN segments use each Gateway, do NOT enable RIP (Routing Information Protocol). Configure the Static Routing table instead. (You also need to configure the other Routers.)
- If using Windows 2000 Data center Server as a software Router, enable RIP on the ADE-4300/ADW-4300, and ensure the following Windows 2000 settings are correct:
 - Open *Routing and Remote Access*
 - In the console tree, select *Routing and Remote Access*, [server name], *IP Routing*, *RIP*
 - In the "Details" pane, right-click the interface you want to configure for RIP version 2, and then click "Properties".
 - On the "General" tab, set *Outgoing packet protocol* to "RIP version 2 broadcast", and *Incoming packet protocol* to "RIP version 1 and 2".

Routing Screen

The routing table is accessed by the *Routing* link on the *Administration* menu.

Using this Screen

Generally, you will use either RIP (Routing Information Protocol) OR the Static Routing Table, as explained above, although it is possible to use both methods simultaneously.

Static Routing Table

- If RIP is not used, an entry in the routing table is required for each LAN segment on your Network, other than the segment to which this device is attached.
- The other Routers must also be configured. See *Configuring Other Routers on your LAN* later in this chapter for further details and an example.

Routing

RIP

Static Routing

RIP Direction

None

RIP Version

RIP-1

Static Routing Table Entries

Add

Edit

Delete

Save

Cancel

Help

Figure 90: Routing Screen

Data - Routing Screen

RIP	
RIP Direction	Select the desired RIP Direction.
RIP Version	Choose the RIP Version for the Server.
Static Routing	
Static Routing Table Entries	<div>This list shows all entries in the Routing Table.<ul style="list-style-type: none">This area shows details of the selected item in the list.Change any the properties as required, then click the "Edit" button to save the changes to the selected entry.</div>
Buttons	
Add	Add a new entry to the Static Routing table, using the data shown in the "Properties" area on screen. The entry selected in the list is ignored, and has no effect.
Edit	Update the current Static Routing Table entry, using the data shown in the table area on screen.
Delete	Delete the current Static Routing Table entry.
Save	Save the RIP setting. This has no effect on the Static Routing Table.

Configuring Other Routers on your LAN

It is essential that all IP packets for devices not on the local LAN be passed to the ADE-4300/ADW-4300, so that they can be forwarded to the external LAN, WAN, or Internet. To achieve this, the local LAN must be configured to use the ADE-4300/ADW-4300 as the *Default Route* or *Default Gateway*.

Local Router

The local router is the Router installed on the same LAN segment as the ADE-4300/ADW-4300. This router requires that the *Default Route* is the ADE-4300/ADW-

4300 itself. Typically, routers have a special entry for the *Default Route*. It should be configured as follows.

Destination IP Address	Normally 0.0.0.0, but check your router documentation.
Network Mask	Normally 0.0.0.0, but check your router documentation.
Gateway IP Address	The IP Address of the ADE-4300/ADW-4300.
Metric	1

Other Routers on the Local LAN

Other routers on the local LAN must use the ADE-4300/ADW-4300's *Local Router* as the *Default Route*. The entries will be the same as the ADE-4300/ADW-4300's local router, with the exception of the *Gateway IP Address*.

- For a router with a direct connection to the ADE-4300/ADW-4300's local Router, the *Gateway IP Address* is the address of the ADE-4300/ADW-4300's local router.
- For routers which must forward packets to another router before reaching the ADE-4300/ADW-4300's local router, the *Gateway IP Address* is the address of the intermediate router.

Static Routing - Example

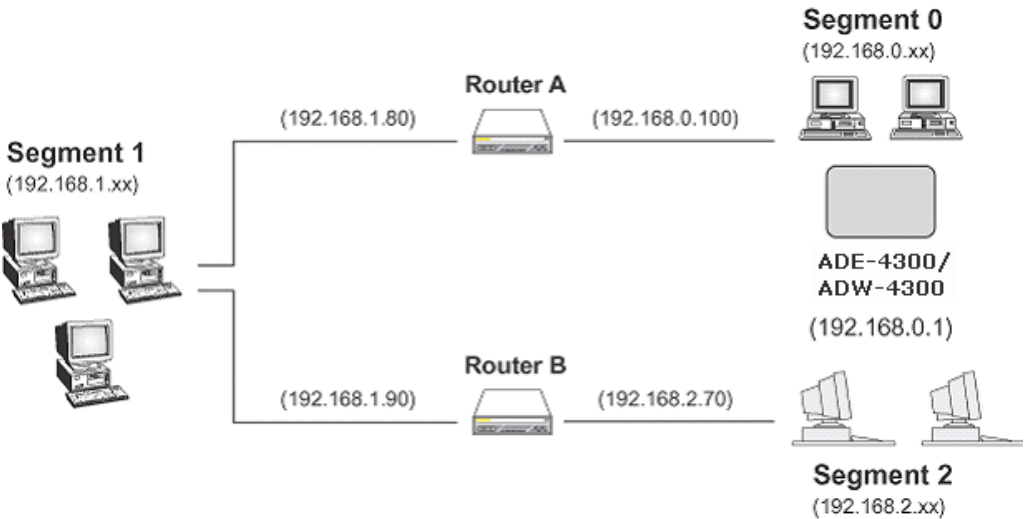


Figure 91: Routing Example

For the ADE-4300/ADW-4300's Routing Table

For the LAN shown above, with 2 routers and 3 LAN segments, the ADE-4300/ADW-4300 requires 2 entries as follows.

Entry 1 (Segment 1)	
Destination IP Address	192.168.1.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.0.100 (ADE-4300/ADW-4300's

	local Router)
Metric	2
Entry 2 (Segment 2)	
Destination IP Address	192.168.2.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.0.100
Metric	3

For Router A's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.0.1 (ADE-4300/ADW-4300's IP Address)

For Router B's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.1.80 (ADE-4300/ADW-4300's local router)

Upgrade Firmware

The firmware (software) in the ADE-4300/ADW-4300 can be upgraded using your Web Browser.

You must first download the upgrade file, then select *Upgrade Firmware* on the *Administration* menu. You will see a screen like the following.

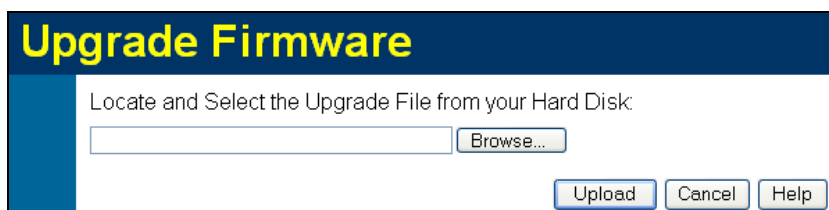


Figure 92: Router Upgrade Screen

To perform the Firmware Upgrade:

1. Click the *Browse* button and navigate to the location of the upgrade file.
4. Select the upgrade file. Its name will appear in the *Upgrade File* field.
5. Click the *Upload* button to commence the firmware upgrade.



Note!

The ADE-4300/ADW-4300 is unavailable during the upgrade process, and must restart when the upgrade is completed. Any connections to or through the ADE-4300/ADW-4300 will be lost.

Chapter 8



Modem Mode

This Chapter explains configuration and operation when in "Modem" or "Bridge" mode..

Overview

There are two modes available on the **Mode** screen.

- **Router** - Both the ADSL Modem and the Router features are operational. In this mode, this device can provide shared Internet Access to all your LAN users. Also, by default, it acts a DHCP Server, providing an IP address and related information to all Wireless (ADW-4300 only) and LAN users.
- **Modem** - Only the ADSL Modem component is operational. All Router features are disabled. This device is "transparent" - it does not perform any operations or make any changes to the network traffic passing through it. You need to have a DHCP Server on your LAN to provide IP addresses to the Wireless clients using this Access Point (ADW-4300 only).

This Chapter describes operation while in **Modem Mode**, also called **Bridge Mode**.

Management Connections

When this device restarts in Modem mode, the IP address does not change, but the DHCP server is disabled. However, your PC will usually retain the IP address provided by the DHCP Server, so the connection will be automatically re-established. You then need to ensure that the IP address of this modem is suitable for your LAN.

- You need to have a DHCP Server on your LAN to provide IP addresses to the Wireless clients using this Access Point (ADW-4300 only).
- This Modem/AP (ADW-4300 only) must be a valid device on your LAN, to allow management connections. You must assign a (fixed) IP address which is within the address range used on your LAN, but not within the address range used by your DHCP server.

When you connect in future, just connect normally, using the IP address you assigned.

1. Start your WEB browser.
- 6 In the *Address* box, enter "HTTP://" and the current IP Address of the ADE-4300/ADW-4300, as in this example, which uses the ADE-4300/ADW-4300's default IP Address:
`HTTP://192.168.0.1`
- 7 When prompted for the User name and Password, enter `admin` for the user name, and the current password, as set on the password screen. (The password is the same regardless of the mode.)

Home Screen

If in Modem mode, the home screen will look like the example below.

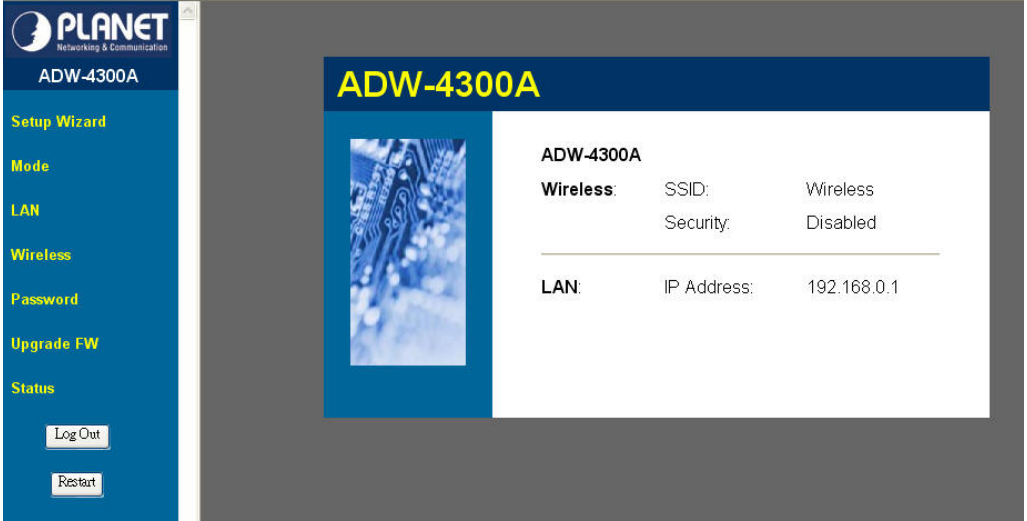


Figure 93: Home Screen - Modem Mode

Note that the menu has changed, many of the options in Router mode are not available. The screens available are:

- **Mode** - change back to Router mode, if desired.
- **LAN** - set IP address, mask and gateway. This is the same as in Router mode, except that the DHCP server is not available while in Modem mode.
- **Wireless (ADW-4300 only)** - this screen, and related sub-screens, is the same as in Router mode.
- **Password** - this screen is the same as in Router mode.
- **Upgrade Firmware** - this screen is the same as in Router mode.
- **Status** - displays current settings and status. See the following section for details.

Mode Screen

This screen is change back to Router mode, if desired.

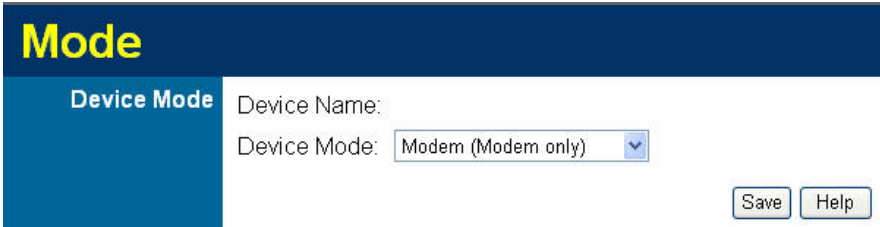


Figure 94: Mode Screen

Data - Mode Screen

Device Name	This field displays the current name of this device.
Device Mode	<p>Select the desired device mode for the router:</p> <ul style="list-style-type: none">• Router - Both the ADSL Modem and the Router features are operational. In this mode, this device can provide shared Internet Access to all your LAN users. Also, by default, it acts a DHCP Server, providing an IP address and related information to all Wireless (ADW-4300 only) and LAN users.• Modem - Only the ADSL Modem component is operational. All Router features are disabled. This device is "transparent" - it does not perform any operations or make any changes to the network traffic passing through it. You need to have a DHCP Server on your LAN to provide IP addresses to the Wireless clients using this Access Point (ADW-4300 only). This mode is also called Bridge Mode. <p>After changing the mode, this device will restart, which will take a few seconds. The menu will also change, depending on the mode you are in.</p>

Operation

Operation is automatic and transparent.

- Wireless clients can connect to the Access Point (ADW-4300 only) if they have the correct SSID and security, but they must obtain an IP address from the DHCP Server on your LAN.
- The modem will act like any other ADSL modem. No routing will be performed, and no client login will be done. If a client login is required, it must be performed by your Router/Gateway or by software on your PC.

Status Screen

In Modem mode, the Status screen looks like the example below.

Status - Bridge Mode

ADSL	Modem Status		Connecting
	DownStream Connection Speed		0 kbps
	UpStream Connection Speed		0 kbps
	VC 1 Status		Enabled
	VC 2 Status		Disabled
	VC 3 Status		Disabled
	VC 4 Status		Disabled
ADSL Details			
LAN	IP Address:	192.168.0.1	
	Network Mask:	255.255.255.0	
	MAC Address	00:30:4F:22:44:D6	
Wireless	Name (SSID)	Wireless	
	Region	Europe	
	Channel	11	
	Wireless AP	enable	
	Broadcast Name	enable	
System	Device Name:	ADW-4300A	
	Firmware Version:	4.10.09	
Attached Devices Refresh Screen Help			

Figure 95: Status Screen - Bridge Mode

Data - Status Screen (Bridge Mode)

System	
Device Name	The current name of the Router. This name is also the "hostname" for users with an "@Home" type connection.
Firmware Version	The version of the current firmware installed.
ADSL	
Modem Status	This indicates the status of the ADSL modem component.
DownStream Connection Speed	Displays the speed for the DownStream Connection.
UpStream Connection Speed	If connected, displays the speed for the Up Stream (upload) ADSL Connection.

VC 1 Status VC 2 Status VC 3 Status VC 4 Status	For each VC (Virtual Circuit), the current status is displayed. This will be either "Enabled" or "Disabled".
ADSL Details	Click this button to open a sub-window and view the details of each VC (Virtual Circuit).
LAN	
IP Address	The IP Address of the ADE-4300/ADW-4300.
Network Mask	The Network Mask (Subnet Mask) for the IP Address above.
MAC Address	This shows the MAC Address for the ADE-4300/ADW-4300, as seen on the LAN interface.
Wireless (ADW-4300 only)	
Name (SSID)	If using an ESS (Extended Service Set, with multiple access points) this ID is called an ESSID (Extended Service Set Identifier).
Region	The current region, as set on the Wireless screen.
Channel	This shows the Channel currently used, as set on the Wireless screen.
Wireless AP	This indicates whether or not the Wireless Access Point feature is enabled.
Broadcast Name	This indicates whether or not the SSID is Broadcast. This setting is on the Wireless screen.
Associated Devices	Clicking this will generate a list of all devices currently using the Access Point.
Buttons	
ADSL Details	View the details of each VC (Virtual Circuit).
Associated Devices	Clicking this will generate a list of all devices currently using the Access Point.
Refresh Screen	Update the data displayed on screen.

Appendix A

Troubleshooting



This Appendix covers the most likely problems and their solutions.

Overview

This chapter covers some common problems that may be encountered while using the ADE-4300/ADW-4300 and some possible solutions to them. If you follow the suggested steps and the ADE-4300/ADW-4300 still does not function properly, contact your dealer for further advice.

General Problems

Problem 1: Can't connect to the ADE-4300/ADW-4300 to configure it.

Solution 1: Check the following:

- The ADE-4300/ADW-4300 is properly installed, LAN connections are OK, and it is powered ON.
- Ensure that your PC and the ADE-4300/ADW-4300 are on the same network segment. (If you don't have a router, this must be the case.)
- If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.
- If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address within the range 192.168.0.2 to 192.168.0.254 and thus compatible with the ADE-4300/ADW-4300's default IP Address of 192.168.0.1.
Also, the Network Mask should be set to 255.255.255.0 to match the ADE-4300/ADW-4300.
In Windows, you can check these settings by using *Control Panel-Network* to check the *Properties* for the TCP/IP protocol.

Internet Access

Problem 1: When I enter a URL or IP address I get a time out error.

Solution 1: A number of things could be causing this. Try the following troubleshooting steps.

- Check if other PCs work. If they do, ensure that your PCs IP settings are correct. If using a Fixed (Static) IP Address, check the Network Mask, Default gateway and DNS as well as the IP Address.
- If the PCs are configured correctly, but still not working, check the ADE-4300/ADW-4300. Ensure that it is connected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.)

- Check the ADE-4300/ADW-4300's status screen to see if it is working correctly.

Problem 2: Some applications do not run properly when using the ADE-4300/ADW-4300.

Solution 2: The ADE-4300/ADW-4300 processes the data passing through it, so it is not transparent.

For incoming connections, you must use the Virtual Server or Firewall Rules to specify the PC which will receive the incoming traffic.

You can also use the *DMZ* function. This should work with almost every application, but:

- It is a security risk, since the firewall is disabled.
- Only one (1) PC can use this feature.

Wireless Access (ADW-4300 only)

Problem 1: My PC can't locate the Wireless Access Point.

Solution 1: Check the following.

- Your PC is set to *Infrastructure Mode*. (Access Points are always in *Infrastructure Mode*)
- The SSID on your PC and the Wireless Access Point are the same.
Remember that the SSID is case-sensitive. So, for example "Workgroup" does NOT match "workgroup".
- Both your PC and the ADW-4300 must have the same setting for WEP. The default setting for the ADW-4300 is disabled, so your wireless station should also have WEP disabled.
- If WEP is enabled on the ADW-4300, your PC must have WEP enabled, and the key must match.
- If the ADW-4300's *Wireless* screen is set to *Allow Trusted PCs only*, then each of your Wireless stations must have been designated as "Trusted", or the Wireless station will be blocked.
- To see if radio interference is causing a problem, see if connection is possible when close to the ADW-4300.
Remember that the connection range can be as little as 100 feet in poor environments.

Problem 2: Wireless connection speed is very slow.

Solution 2: The wireless system will connect at the highest possible speed, depending on the distance and the environment. To obtain the highest possible connection speed, you can experiment with the following:

- ADW-4300 location.
Try adjusting the location and orientation of the ADW-4300.
- Wireless Channel
If interference is the problem, changing to another channel may show a marked improvement.
- Radio Interference
Other devices may be causing interference. You can experiment by switching other devices Off, and see if this helps. Any "noisy"

devices should be shielded or relocated.

- RF Shielding

Your environment may tend to block transmission between the wireless stations. This will mean high access speed is only possible when close to the ADW-4300.

Appendix B



About Wireless LANs_(ADW-4300 only)

This Appendix provides some background information about using Wireless LANs (WLANs).

Modes

Wireless LANs can work in either of two (2) modes:

- Ad-hoc
- Infrastructure

Ad-hoc Mode

Ad-hoc mode does not require an Access Point or a wired (Ethernet) LAN. Wireless Stations (e.g. notebook PCs with wireless cards) communicate directly with each other.

Infrastructure Mode

In Infrastructure Mode, one or more Access Points are used to connect Wireless Stations (e.g. Notebook PCs with wireless cards) to a wired (Ethernet) LAN. The Wireless Stations can then access all LAN resources.



Access Points can only function in "Infrastructure" mode, and can communicate only with Wireless Stations which are set to "Infrastructure" mode.

BSS/ESS

BSS

A group of Wireless Stations and a single Access Point, all using the same ID (SSID), form a Basic Service Set (BSS).

Using the same SSID is essential. Devices with different SSIDs are unable to communicate with each other.

ESS

A group of Wireless Stations, and multiple Access Points, all using the same ID (ESSID), form an Extended Service Set (ESS).

Different Access Points within an ESS can use different Channels. In fact, to reduce interference, it is recommended that adjacent Access Points **SHOULD** use different channels.

As Wireless Stations are physically moved through the area covered by an ESS, they will automatically change to the Access Point which has the least interference or best

performance. This capability is called **Roaming**. (Access Points do not have or require Roaming capabilities.)

Channels

The Wireless Channel sets the radio frequency used for communication.

- Access Points use a fixed Channel. You can select the Channel used. This allows you to choose a Channel which provides the least interference and best performance. In the USA and Canada, 11 channels are available. If using multiple Access Points, it is better if adjacent Access Points use different Channels to reduce interference.
- In "Infrastructure" mode, Wireless Stations normally scan all Channels, looking for an Access Point. If more than one Access Point can be used, the one with the strongest signal is used. (This can only happen within an ESS.)
- If using "Ad-hoc" mode (no Access Point), all Wireless stations should be set to use the same Channel. However, most Wireless stations will still scan all Channels to see if there is an existing "Ad-hoc" group they can join.

WEP

WEP (Wired Equivalent Privacy) is a standard for encrypting data before it is transmitted.

This is desirable because it is impossible to prevent snoopers from receiving any data which is transmitted by your Wireless Stations. But if the data is encrypted, then it is meaningless unless the receiver can decrypt it.

If WEP is used, the Wireless Stations and the Access Point must have the same settings for each of the following:

WEP	Off, 64 Bit, 128 Bit
Key	For 64 Bit encryption, the Key value must match. For 128 Bit encryption, the Key value must match
WEP Authentication	Open System or Shared Key.

WPA-PSK

WPA-PSK is another standard for encrypting data before it is transmitted. This is a later standard than WEP (Wired Equivalent Privacy), and provides greater security for your data. Data is encrypted using a 256Bit key which is automatically generated and changed often.

If all your Wireless stations support WPA-PSK, you should use this instead of WEP.

If WPA-PSK is used, the Wireless Stations and the Access Point must have the same settings for each of the following:

WPA PSK (Pre-shared Key)	Enter the same value on every station and the AP. The PSK must be from 8 to 63 characters in length. The 256Bit key used for the actual encryption is derived from this key.
-------------------------------------	--

Encryption	The same encryption method must be used. The most common encryption method is TKIP. Another widely-supported method is AES.
-------------------	---

Wireless LAN Configuration

To allow Wireless Stations to use the Access Point, the Wireless Stations and the Access Point must use the same settings, as follows:

Mode	On client Wireless Stations, the mode must be set to "Infrastructure". (The Access Point is always in "Infrastructure" mode.)
SSID (ESSID)	Wireless Stations should use the same SSID (ESSID) as the Access Point they wish to connect to. Alternatively, the SSID can be set to "any" or null (blank) to allow connection to any Access Point.
Wireless Security	<p>The Wireless Stations and the Access Point must use the same settings for Wireless security. (None, WEP, WPA-PSK).</p> <p>WEP: If WEP is used, the Key size (64Bit, 128Bit), Key value, and Authentication settings must be the same on the Wireless Stations and the Access Point.</p> <p>WPA-PSK: If WPA-PSK is used, all Wireless Stations must be set to use WPA-PSK, and have the same Pre-shared Key and encryption system.</p> <p>For Ad-hoc networks (no Access Point), all Wireless stations must use the same security settings.</p>

Appendix C

About VPNs



Overview

A VPN (Virtual Private Network) provides a secure connection between 2 points, over an insecure network - typically the Internet. This secure connection is called a **VPN Tunnel**.

There are many standards and protocols for VPNs. The standard implemented in the ADE-4300/ADW-4300 is **IPSec**.

IPSec

IPSec is a near-ubiquitous VPN security standard, designed for use with TCP/IP networks. It works at the packet level, and authenticates and encrypts all packets traveling over the VPN Tunnel. Thus, it does not matter what applications are used on your PC. Any application can use the VPN like any other network connection.

IPsec VPNs exchange information through logical connections called **SAs** (Security Associations). An SA is simply a definition of the protocols, algorithms and keys used between the two VPN devices (endpoints).

Each IPsec VPN has two SAs - one in each direction. If **IKE** (Internet Key Exchange) is used to generate and exchange keys, there are also SA's for the IKE connection as well as the IPsec connection.

There are two security modes possible with IPSec:

- **Transport Mode** - the payload (data) part of the packet is encapsulated through encryption but the IP header remains in the clear (unchanged).
The ADE-4300/ADW-4300 does NOT support Transport Mode.
- **Tunnel Mode** - everything is encapsulated, including the original IP header, and a new IP header is generated. Only the new header is in the clear (i.e. not protected). This system provides enhanced security.

The ADE-4300/ADW-4300 always uses Tunnel Mode.

IKE

IKE (Internet Key Exchange) is an optional, but widely used, component of IPsec. IKE provides a method of negotiating and generating the keys and IDs required by IPsec. If using IKE, only a single key is required to be provided during configuration. Also, IKE supports using **Certificates** (provided by CAs - Certification Authorities) to authenticate the identity of the remote user or gateway.

If IKE is NOT used, then all keys and IDs (SPIs) must be entered manually, and Certificates can NOT be used. This is called a "Manual Key Exchange".

When using IKE, there are 2 phases to creating the VPN tunnel:

- **Phase I** is the negotiation and establishment up of the IKE connection.
- **Phase II** is the negotiation and establishment up of the IPsec connection.

Because the IKE and IPsec connections are separate, they have different SAs (security associations).

Policies

VPN configuration settings are stored in **Policies**.

Note that different vendors use different terms. Generally, the terms "VPN Policy", "IPSec Policy", and "IPSec Proposal" have the same meaning. However, some vendors separate IKE Policies (Phase 1 parameters) from IPSec Policies (Phase 2 parameters).

For the ADE-4300/ADW-4300; each VPN policy contains both Phase 1 and Phase 2 parameters (if IKE is used). Each policy defines:

- The address of the remote VPN endpoint
- The traffic which is allowed to use the VPN connection.
- The parameters (settings) for the IPsec SA (Security Association)
- If IKE is used, the parameters (settings) for the IKE SA (Security Association)

Generally, you will need at least one (1) VPN Policy for each remote site for which you wish to establish VPN connections.

It is possible, and sometimes necessary, to have multiple Policies for the same remote site. However, you should only Enable one (1) policy at a time.

VPN Configuration

The general rule is that each endpoint must have matching Policies, as follows:

VPN Endpoint address	<p>Each VPN endpoint must be configured to initiate or accept connections to the remote VPN client or Gateway.</p> <p>Usually, this requires having a fixed Internet IP address. However, it is possible for a VPN Gateway to accept incoming connections from a remote client where the client's IP address is not known in advance.</p>
Local & Remote LAN definition	<p>This determines which outgoing traffic will cause a VPN connection to be established, and which incoming traffic will be accepted. Each endpoint must be configured to pass and accept the desired traffic from the remote endpoint.</p> <p>If connecting 2 LANs, this requires that:</p> <ul style="list-style-type: none">• Each endpoint must be aware of the IP addresses used on the other endpoint.• The 2 LANs MUST use different IP address ranges.
IKE parameters	<p>If using IKE (recommended), the IKE parameters must match (except for the SA lifetime, which can be different).</p>
IPsec parameters	<p>The IPsec parameters at each endpoint must match.</p>

Common VPN Situations

VPN Pass-through

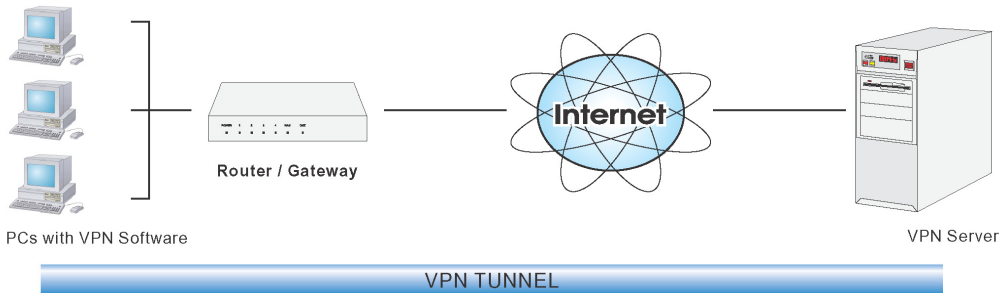


Figure 96: VPN Pass-through

Here, a PC on the LAN behind the Router/Gateway is using VPN software, but the Router/Gateway is NOT acting as a VPN endpoint. It is only allowing the VPN connection.

- The PC software can use any VPN protocol supported by the remote VPN.
- The remote VPN Server must support client PCs which are behind a NAT router, and so have an IP address which is not valid on the Internet.
- The Router/Gateway requires no VPN configuration, since it is not acting as a VPN endpoint.

Client PC to VPN Gateway

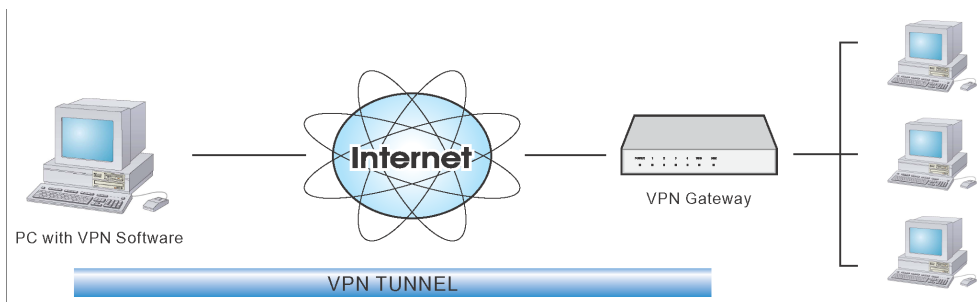


Figure 97: Client PC to VPN Server

In this situation, the PC must run appropriate VPN client software in order to connect, via the Internet, to the ADE-4300/ADW-4300 or other VPN Gateway. Once connected, the client PC has the same access to LAN resources as PCs on the local LAN (unless restricted by the network administrator).

- IPsec is not the only protocol which can be used in this situation, but the ADE-4300/ADW-4300 supports IPsec ONLY.
- Windows 2000 and Windows XP include an IPsec VPN client program. However, configuration of this client program for use with the ADE-4300/ADW-4300 is very complex and beyond the scope of this document.

Connecting 2 LANs via VPN

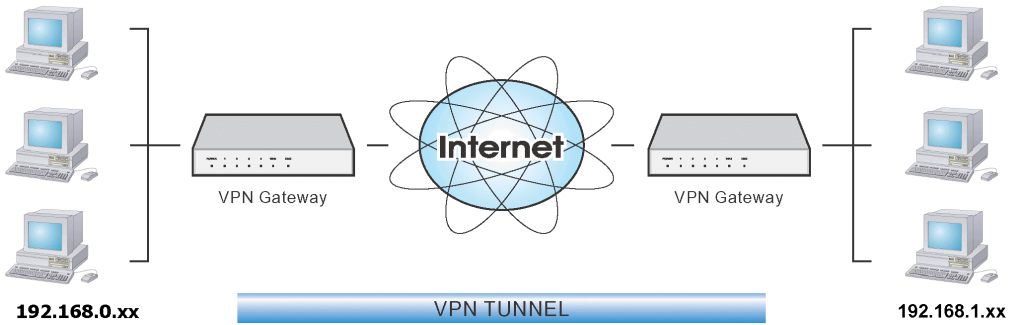


Figure 98: Connecting 2 VPN Gateways

This allows two (2) LANs to be connected. PCs on each endpoint gain secure access to the remote LAN.

- The 2 LANs MUST use different IP address ranges.
- The VPN Policies at each end determine when a VPN tunnel will be established, and what systems on the remote LAN can be accessed once the VPN connection is established.
- It is possible to have simultaneous VPN connections to many remote sites.

VPN Example

In this example, 2 LANs are connected via VPN. Each end has a ADE-4300/ADW-4300.

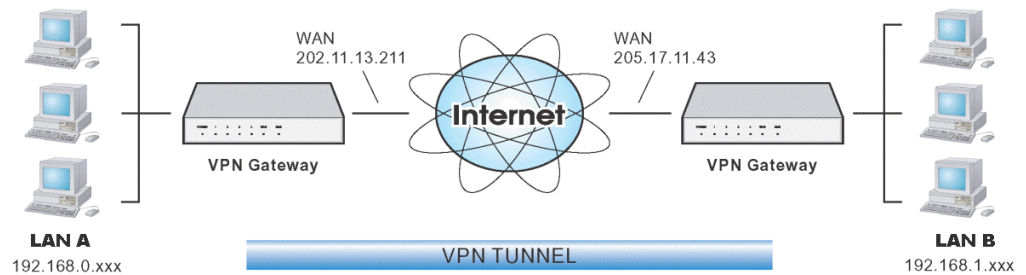


Figure 99: Connecting 2 ADE-4300/ADW-4300s

Note

- The LANs MUST use different IP address ranges.
- Both endpoints have fixed WAN (Internet) IP addresses.
- This example uses an "Auto" policy, using IKE

Configuration Settings - Gateway A

Gateway A should be configured as shown below.

VPN - Auto Policy

General

Policy Name:

Remote VPN Endpoint

Address Type:

Address Data:

☒ NetBIOS Enable

Local LAN

IP Address

IP address: . . .

Subnet Mask: . . .

Remote LAN

IP Address

IP address: . . .

Subnet Mask: . . .

IKE

Direction

Exchange Mode

Diffie-Hellman (DH) Group

Local Identity Type

Data

Remote Identity Type

Data

SA Parameters

Encryption:

Authentication:

Pre-shared Key:

SA Life Time:

(Seconds)

☐ Enable PFS (Perfect Forward Security)

Back

Save

Cancel

Help

Figure 100: Gateway A Configuration

132

Configuration Settings - Gateway B

Gateway B should be configured as shown below.

VPN - Auto Policy

General	Policy Name: <input style="width: 150px;" type="text" value="Example"/> Remote VPN Endpoint Address Type: <input style="width: 100px;" type="text" value="Fixed IP Address"/> Address Data: <input style="width: 100px;" type="text" value="202.11.13.211"/> <input checked="" type="checkbox"/> NetBIOS Enable
Local LAN	IP Address <input style="width: 50px;" type="text" value="Subnet address"/> IP address: <input style="width: 30px;" type="text" value="192"/> . <input style="width: 30px;" type="text" value="168"/> . <input style="width: 30px;" type="text" value="1"/> . <input style="width: 30px;" type="text" value="1"/> Subnet Mask: <input style="width: 30px;" type="text" value="255"/> . <input style="width: 30px;" type="text" value="255"/> . <input style="width: 30px;" type="text" value="255"/> . <input style="width: 30px;" type="text" value="0"/>
Remote LAN	IP Address <input style="width: 50px;" type="text" value="Subnet address"/> IP address: <input style="width: 30px;" type="text" value="192"/> . <input style="width: 30px;" type="text" value="168"/> . <input style="width: 30px;" type="text" value="0"/> . <input style="width: 30px;" type="text" value="1"/> Subnet Mask: <input style="width: 30px;" type="text" value="255"/> . <input style="width: 30px;" type="text" value="255"/> . <input style="width: 30px;" type="text" value="255"/> . <input style="width: 30px;" type="text" value="0"/>
IKE	Direction: <input style="width: 100px;" type="text" value="Initiator and Responder"/> Exchange Mode: <input style="width: 50px;" type="text" value="Main Mode"/> Diffie-Hellman (DH) Group: <input style="width: 100px;" type="text" value="Group 2 (1024 Bit)"/> Local Identity Type: <input style="width: 100px;" type="text" value="WAN IP Address"/> Data: <input style="width: 100px;" type="text" value="n/a"/> Remote Identity Type: <input style="width: 100px;" type="text" value="IP Address"/> Data: <input style="width: 100px;" type="text" value="n/a"/>
SA Parameters	Encryption: <input style="width: 50px;" type="text" value="3DES"/> Authentication: <input style="width: 50px;" type="text" value="MD5"/> Pre-shared Key: <input style="width: 150px;" type="text" value="12345678"/> SA Life Time: <input style="width: 50px;" type="text" value="28800"/> (Seconds) <input type="checkbox"/> Enable PFS (Perfect Forward Security)

Figure 101: Gateway B Configuration

Settings

Setting	LAN A Gateway	LAN B Gateway	Notes
Policy Name	Example	Example	Name does not affect operation. Select a meaningful name.
Remote VPN Endpoint	Fixed IP Address 205.17.11.43	Fixed IP Address 202.11.13.211	Other endpoint's WAN (Internet) IP address.

NetBIOS	Enable	Enable	Disable if not required.
Local LAN IP address Mask	192.168.0.1 255.255.255.0	192.168.1.1 255.255.255.0	Local Address subnet. Use a more restrictive definition if possible.
Remote LAN IP address Mask	192.168.1.1 255.255.255.0	192.168.0.1 255.255.255.0	Remote Address subnet. Use a more restrictive definition if possible.

IKE

Direction	Initiator & responder	Initiator & responder	Does not have to match. Either endpoint can block 1 direction.
Exchange mode	Main Mode	Main Mode	Must match
DH Group	Group 2 (1024 bit)	Group 2 (1024 bit)	Must match
Local Identity	IP address	IP address	IP address is the most common ID method
Remote Identity	WAN IP address	WAN IP address	IP address is the most common ID method

SA Parameters

Encryption	3DES	3DES	Must match.
Authentication	MD5	MD5	Must match
Pre-shared Key	12345678	12345678	Must match; use any string.
SA Life time	28800	28800	Does not have to match. Shorter period will be used.
PFS	Disabled	Disabled	Must match

Note:

Some VPN Gateways or programs let you specify the following settings separately for IKE and IPSec. For this device, the same settings are used for both IKE and IPSec.

- Authentication
- Encryption
- SA Lifetime

Also, IPSec allows for "AH Authentication", using MD5 or SHA-1. For this device, "AH Authentication" is always DISABLED.

Appendix D

Specifications



ADSL 2/2+ VPN Firewall Router

Product		ADSL 2/2+ VPN Firewall Router, 802.11g Wireless ADSL 2/2+ VPN Firewall Router
Model		ADE-4300A/B, ADW-4300A/B
Hardware		
Standard		Multi-Mode code support ANSI T1.413 Issue 2 ITU-T G.994.1 (G.hs) rev. 3 ITU-T G.992.1(G.dmt) - Annex A (ADSL over POTS for ADW-4300A) - Annex B (ADSL over ISDN for ADW-4300B) ITU-T G.992.2(G.lite) ITU-T G.992.3 Annex A ADSL2 ITU-T G.992.3 Annex A DELT ITU-T G.992.3 Annex L READSL2 ITU-T G.992.5 Annex A ADSL2+
Protocol		RFC 2364 - PPP over ATM (LLC/VCMUX) RFC 2516 - PPP over Ethernet (LLC/VCMUX) RFC 1577 - Classic IP over ATM (LLC/VCMUX) RFC 1483 - Bridged IP over ATM (LLC/VCMUX) RFC 1483 - Routed IP over ATM (LLC/VCMUX)
AAL and ATM Support		Integrated ATM AAL5 support 255 VPI plus 65535 VCI address range
Ports	LAN	4 (10Base-T/100Base-TX, Auto-Negotiation, Auto MDI/MDI-X)
	Wireless(ADW-4300 only)	1 x 802.11g wireless access point, antenna detachable
	WAN	1 (RJ-11, 10/100Base-TX, Auto-Negotiation)
LED Indicators		PWR, STATUS, WLAN (ADW-4300 only), ADSL 100 LNK/ACT, 10 LNK ACT for each LAN port
Button		1 for reset/factory reset
Software		
Protocol		IP, NAT, ARP, ICMP, DHCP, PPPoE, PPPoA, IPoA, RIP1/2, SNMPv1
Security		Native NAT firewall, Enhanced policy-based+ SPI firewall, URL Filter, Blocking log, Virtual Server, DMZ, Access Control
VPN termination		IPSec tunnel 8 simultaneous tunnels (Main Mode) Throughput 1.5Mbps DES/3DES encryption IKE support with pre-shared key IP address or FQDN identification MD5, SHA-1 Authentication PPTP Server (Microsoft VPN) support

Management	Web browser management
Environment Specification	
Dimension (W x D x H)	199 mm x 150 mm x 33 mm
Power	15V AC, 1A
Power Consumption	Maximum 15W, 51 BTU
Temperature:	0~40 degree C (operating), -10~70 degree C (storage)
Humidity	5%~ 95% (non-condensing)
Emission	FCC, CE

Wireless Interface (ADW-4300 only)

Standards	IEEE802.11b, IEEE802.11g WLAN, 802.11G-plus (Texas Instruments proprietary enhanced mode)
Frequency	2.4 to 2.4835GHz (Industrial Scientific Medical Band)
Channels	Maximum 14 Channels, depending on regulatory authorities
Modulation	CCK, DQPSK, DBPSK, OFDM/CCK
Data Rate	Up to 54 Mbps (802.11g), 64 Mps (TI 802.11G-plus)
Security	WEP 64Bit 、128Bit, WPA-PSK, MAC address checking
Output Power	13dBm (typical)
Receiver Sensitivity	-80dBm Min.

Regulatory Approvals

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) This device must accept any interference received, including interference that may cause undesired operation.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

CE Approval

CE Standards

This product complies with the 99/5/EEC directives, including the following safety and EMC standards:

- EN300328-2
- EN301489-1/-17
- EN60950

CE Marking Warning

This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.